Elementary Number Theory

A revision by Jim Hefferon, St Michael's College, 2003-Dec
of notes by W. Edwin Clark, University of South Florida, 2002-Dec

LaTeX source compiled on January 5, 2004 by Jim Hefferon, jim@joshua.smcvt.edu.

Preface

Mathematics is the queen of sciences and arithmetic the queen of mathematics

Carl Friedrich Gauss

Number theory, known to Gauss as "arithmetic," studies the properties of the integers: $\ldots -3, -2, -1, 0, 1, 2, 3 \ldots$. Although the integers are familiar, and their properties might therefore seem simple, it is instead a very deep subject.

For example, here are some problems in number theory that remain unsolved. (Recall that a *prime number* is an integer greater than 1 whose only positive factors are 1 and the number itself.) Note that these problems are simple to state — just because a topic is accessibile does not mean that it is easy.

1. (*Goldbach's Conjecture*) Is every even integer $n > 2$ the sum of two primes?

2. (*Twin Prime Conjecture*) Are there are infinitely many twin primes? (*Twin primes* differ by 2, like 11 and 13.)

3. Are there infinitely many primes of the form $n^2 + 1$? Of the form $2^n - 1$? (Ones of this form are *Mersenne primes*.) Of the form $2^{2^n} + 1$? (These are *Fermat primes*.)

4. Are there infinitely many primes whose digits are all 1's? (Numbers of this form are *repunits*.)

5. Are there infinitely many perfect numbers? (An integer is *perfect* if it is the sum of its proper divisors; 6 is perfect because $1 + 2 + 3 = 6$.)

6. ($3n + 1$ *Conjecture*) Consider the function f defined by: $f(n) = 3n + 1$ if n is odd and $f(n) = n/2$ if n is even. Does the sequence of iterates $f(n)$, $f(f(n))$, $f(f(f(n)))$, $\ldots$ always contain 1, no matter what starting value n is used?

7. Is there a fast algorithm for factoring large integers?

So the subject is not simple. However it is accessible, and beautiful.

A caution In some areas a person needs to learn by starting from first principles. The first course in Calculus is like that; students learn limits first to avoid getting nutty ideas about nx^{n-1}, But other areas are best mastered by diving right in.

In this book you dive into mathematical arguments. Number Theory is right for this in part because of its accessibility.

But always keep in mind the caution: do not underestimate the material. You will find this subject hard, albiet rewarding.

Prerequisites We require only Calculus I. Even that requirement is not strict (limits come up, as do the rules of logarithm manipultion), so the main purpose of the prerequisite is that we expect that with it comes a certain amount of mathematical maturity, including familiarity with basic set theory and some function facts.

Other resources The Internet contains much interesting and current information about number theory; see the Bibliography. The websites by Chris Caldwell [2] and by Eric Weisstein [13] are especially good. To see what is going on at the frontier of the subject, you may take a look at some recent issues of the *Journal of Number Theory* which you will find in any university library.

Contents

Chapter 1

Divisibility

In this book, all numbers are integers, unless specified otherwise. Thus in the next definition, d, n, and k are integers.

1.1 Definition The number d *divides* the number n if there is a k such that $n = dk$. (Alternate terms are: d is a *divisor* of n, or d is a *factor* of n, or n is a *multiple* of d.) This relationship between d and n is symbolized $d \mid n$. The symbol $d \nmid n$ means that d does not divide n.

Note that the symbol $d \mid n$ is different from the fraction symbol d/n. It is also different from n/d because $d \mid n$ is either true or false, while n/d is a rational number.

1.2 Theorem (Divisibility Properties) For all numbers n, m, and d,

(1) $d \mid 0$
(2) $0 \mid n \implies n = 0$
(3) $1 \mid n$
(4) *(Reflexivity property)* $n \mid n$
(5) $n \mid 1 \implies n = 1$ or $n = -1$
(6) *(Transitivity property)* $d \mid n$ and $n \mid m \implies d \mid m$
(7) *(Multiplication property)* $d \mid n \implies ad \mid an$
(8) *(Cancellation property)* $ad \mid an$ and $a \neq 0 \implies d \mid n$
(9) *(Linearity property)* $d \mid n$ and $d \mid m \implies d \mid an + bm$ for all a and b
(10) *(Comparison property)* If d and n are positive and $d \mid n$ then $d \leq n$

PROOF. For the first item, take $k = 0$. For the second, if $0 \mid n$ then $n = 0 \cdot k = 0$.

The next item holds because we can take n as the k in the definition. Reflexivity is similar: $n = n \cdot 1$ shows that it holds. The next property follows immediately from Basic Axiom 3 for $\mathbb{Z}$, from the first Appendix.

For Transitivity, assume the $d \mid n$ and that $n \mid m$. Then $n = dk_1$ and $m = nk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Substitute to get $m = nk_2 = (dk_1)k_2$. By the Associative Property of Multiplication, $(dk_1)k_2 = d(k_1k_2)$, which shows that d divides m.

Multiplication also follows from associativity. Assume that $d \mid n$ so that $n = dk$. Then $an = a(dk) = (ad)k$ shows that $ad \mid ak$.

For Cancellation, assume that $a \neq 0$ and that $ad \mid an$. Then there is a k such that $an = (ad)k$. We will show that $n = dk$. Assume first that $a > 0$. By the Trichotomy Property from the first Appendix, either $n > dk$ or $n = dk$ or $n < dk$. If $n > dk$ then we have that $an > a(dk) = (ad)k$, which contradicts this paragraph's assumption that $an = (ad)k$. If $n < dk$ then $an < a(dk) = (ad)k$, also contradicting the assumption. Therefore $n = dk$, and so $d \mid n$. The argument for the $a < 0$ case is similar.

To verify Linearity, suppose that $d \mid n$ and $d \mid m$ so that $n = dk_1$ and $m = dk_2$ for $k_1, k_2 \in \mathbb{Z}$. Then $an + bm = a(dk_1) + b(dk_2) = d(ak_1 + bk_2)$ shows that $d \mid (an + bm)$.

Finally, for Comparison, assume that $d, n > 0$ and $d \mid n$. Then $n = dk$ for some k. Observe that k is positive because the other two are positive. By Trichotomy, either $d < n$ or $d = n$ or $d > n$. We will show that the $d > n$ case is not possible. Assume that $d > n$. Then $dk > nk$ follows by one of the first Appendix's Properties of Inequalities. But that gives $n > nk$, which means that $n \cdot 1 > n \cdot k$ despite that fact that k is positive and so $1 \leq k$. This is impossible because it violates the same Property of Inequalities. QED

1.3 Definition An integer n is *even* (or has *even parity*) if it is divisible by 2 and is *odd* (or is of *odd parity*) otherwise.

1.4 Lemma Recall that $|a|$ equals a if $a \geq 0$ and equals $-a$ if $a < 0$.

(1) If $d \mid a$ then $-d \mid a$ and $d \mid -a$.
(2) If $d \mid a$ then $d \mid |a|$
(3) The largest positive integer that divides a nonzero number a is $|a|$.

PROOF. For (1), if $d \mid a$ then $a = dk$ for some k. It follows that $a = (-d)(-k)$ and since $-d$ and $-k$ are also integers, this shows that $-d \mid a$. It also follows that $-a = (-k)d$, and so $d \mid -a$.

For (2), suppose first that a is nonnegative. Then $|a| = a$ and so if $d \mid a$ then $d \mid |a|$. Next suppose that a is negative. Since $|a| = -a$ for negative a, and since (1) shows that $d \mid -a$, and d therefore divides $|a|$.

For (3), first note that $|a|$ actually divides a: in the $a \geq 0$ case $|a| \mid a$ because in this case $|a| = a$ and we know that $a \mid a$, while in the $a < 0$ case we have that $a = |a|(-1)$, so that $|a|$ is indeed a factor of a. We finish by showing that $|a|$ is maximal among the divisors of a. Suppose that d is a positive number that divides a. Then $a = dk$ for some k, and also $-a = d(-k)$. Thus $d \mid |a|$, whether a is positive or negative. So by the Comparison property of Theorem 1.2, we have that $d \leq |a|$. QED

Chapter 2

Prime Numbers

2.1 Definition An integer $p \geq 2$ is *prime* if it has no positive divisors other than 1 and itself. An integer greater than or equal to 2 that is not prime is *composite*.

Note that 1 is neither prime nor composite.

2.2 Lemma An integer $n \geq 2$ is composite if and only if it has factors a and b such that $1 < a < n$ and $1 < b < n$.

PROOF. Let $n \geq 2$. The 'if' direction is obvious. For 'only if', assume that n is composite. Then it has a positive integer factor a such that $a \neq 1$, $a \neq n$. This means that there is a b with $n = ab$. Since n and a are positive, so is b. Hence $1 \leq a$ and $1 \leq b$. By Theorem 1.2, $a \leq n$ and $b \leq n$. Since $a \neq 1$ and $a \neq n$ we have $1 < a < n$. If $b = 1$ then $a = n$, which is not possible, so $b \neq 1$. If $b = n$ then $a = 1$, which is also not possible. So $1 < b < n$, finishing this half of the argument. QED

2.3 Lemma If $n > 1$ then there is a prime p such that $p \mid n$.

PROOF. Let S denote the set of all integers greater than 1 that have no prime divisor. We must show that S is empty.

If S is not empty then by the Well-Ordering Property it has a smallest member; call it m. Now $m > 1$ and has no prime divisor. Then m cannot be prime (as every number is a divisor of itself). Hence m is composite. Therefore by Lemma 2.2, $m = ab$ where $1 < a < m$ and $1 < b < m$. Since $1 < a < m$, the factor a is not a member of S. So a must have a prime divisor p. Then $p \mid a$ and $a \mid m$, so by Theorem 1.2, $p \mid m$. This contradicts the assumption that m has no prime divisor. So the set S must be empty. QED

2.4 Theorem (Euclid's Theorem) There are infinitely many primes.

PROOF. Assume, to get a contradiction, that there are only a finitely many primes $p_1 = 2, p_2 = 3, \ldots, p_n$. Consider the number $N = p_1 p_2 \cdots p_n + 1$.

Since $p_1 \geq 2$, clearly $N \geq 2$. So by Lemma 2.3, N has a prime divisor p. That prime must be one of $p_1, \ldots, p_n$ since that list was assumed to be exhaustive. However, observe that the equation

$$N = p_i \left(p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n\right) + 1$$

along with $0 \leq 1 < p_i$ shows by Lemma 3.2 that n is not divisible by p_i. This is a contradiction; it follows that the assumption that there are only finitely many primes is not true. QED

2.5 Remark Eucild's Theorem, and its proof, is often cited as an example of the beauty of Mathematics.

2.6 Theorem If $n > 1$ is composite then n has a prime divisor $p \leq \sqrt{n}$.

PROOF. Let $n > 1$ be composite. Then $n = ab$ where $1 < a < n$ and $1 < b < n$. We claim that at least one of a or b is less than or equal to $\sqrt{n}$. For if not then $a > \sqrt{n}$ and $b > \sqrt{n}$, and hence $n = ab > \sqrt{n} \cdot \sqrt{n} = n$, which is impossible.

Suppose, without loss of generality, that $a \leq \sqrt{n}$. Since $1 < a$, by Lemma 2.3 there is a prime p such that $p \mid a$. Hence, by Transitivity in Theorem 1.2, since $a \mid n$ we have $p \mid n$. By Comparison in Theorem 1.2, since $p \mid a$ we have $p \leq a \leq \sqrt{n}$. QED

We can use Theorem 2.6 to help compute whether an integer is prime. Given $n > 1$, we need only try to divide it by all primes $p \leq \sqrt{n}$. If none of these divides n then n must be prime.

2.7 Example Consider the number 97. Note that $\sqrt{97} < \sqrt{100} = 10$. The primes less than 10 are 2, 3, 5, and 7. None of these divides 97, and so 97 is prime.

Chapter 3

Division

3.1 Theorem Where a and $b > 0$ are integers, there are integers q and r, called the *quotient* and the *remainder* on division of a by b, satisfying these two conditions.

$$a = bq + r \qquad 0 \leq r < b$$

Further, those integers are unique.

Note that this result has two parts. One part is that the theorem says there exists a quotient and remainder satisfying the conditions. The second part is that the quotient, remainder pair are unique: no other pair of numbers satisfies those conditions.

PROOF. To verify that for any a and $b > 0$ there exists an appropriate quotient and remainder we need only produce suitable numbers. Consider these.

$$q = \left\lfloor \frac{a}{b} \right\rfloor \qquad r = a - bq$$

Obviously $a = bq + r$, so these satisfy the first condition. To finish the existence half of this proof, we need only check that $0 \leq r < b$. The Floor Lemma from the Some Properties of $\mathbb{R}$ appendix gives

$$\frac{a}{b} - 1 < \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}.$$

Multiply all of the terms of this inequality by $-b$. Since b is positive, $-b$ is negative, and so the direction of the inequality is reversed.

$$b - a > -b \left\lfloor \frac{a}{b} \right\rfloor \geq -a$$

Add a to all three terms of the inequality and replace $\lfloor a/b \rfloor$ by q to get

$$b > a - bq \geq 0.$$

Since $r = a - bq$ this shows that $0 \leq r < b$.

We still must prove that q and r are unique. Assume that there are two quotient, remainder pairs

$$a = bq_1 + r_1 \quad \text{with} \quad 0 \leq r_1 < b$$

and

$$a = bq_2 + r_2 \quad \text{with} \quad 0 \leq r_2 < b.$$

Subtracting

$$0 = a - a = (bq_1 + r_1) - (bq_2 + r_2) = b(q_1 - q_2) + (r_1 - r_2)$$

implies that

$$r_2 - r_1 = b(q_1 - q_2). \tag{3.1}$$

We must show that the two pairs are equal, that $r_1 = r_2$ and $q_1 = q_2$. To obtain a contradiction, suppose otherwise. First suppose that $r_1 \neq r_2$. Then one must be larger than the other; without loss of generality assume that $r_2 > r_1$. Then

$$0 \leq r_1 < r_2 < b$$

and so $r_2 - r_1 < b$. But (3.1) shows that b divides $r_2 - r_1$ and by the Comparison property of Theorem 1.2 this implies that $b \leq r_2 - r_1$. This is the desired contradiction and so we conclude that $r_1 = r_2$. With that, from equation 3.1 we have $0 = b(q_1 - q_2)$. Since $b > 0$, this gives that $q_1 - q_2 = 0$ and so $q_1 = q_2$. QED

3.2 Corollary The number d divides the number n if and only if on division of n by d the remainder is 0.

PROOF. If the remainder is 0 then $n = dq + 0 = dq$ shows that $d \mid n$. For the other half, if $d \mid n$ then for some k we have $n = dk = dk + 0$ (with $0 \leq 0 < d$) and the fact that the quotient, remainder pair is uniqus shows that k and 0 must be the quotient and the remainder. QED

That corollary says that Theorem 3.1 generalizes the results on divisibility. For instance, fix $b = 3$. Then, given a, instead of only being able to say that a is divisible or not, we can give a finer description: a leaves a remainder of 0 (this is the case where $b \mid a$), or 1, or 2.

3.3 Definition For $b > 0$ define $a \bmod b = r$ where r is the remainder when a is divided by b.

For example $23 \bmod 7 = 2$ since $23 = 7 \cdot 3 + 2$ and $-4 \bmod 5 = 1$ since $-4 = 5 \cdot (-1) + 1$.

Chapter 4

Greatest Common Divisor

4.1 Definition An integer is a *common divisor* of two others if it divides both of them.

We write $\mathcal{C}(a, b)$ for the set of numbers that are common divisors of a and b.

4.2 Definition The *greatest common divisor* of two nonzero integers a and b, $\gcd(a, b)$, is the largest integer that divides both, except that $\gcd(0, 0) = 0$.

The exception is there because every number divides zero, and so we specially define $\gcd(0, 0)$ to be a convienent value.

4.3 Example The set of common divisors of 18 and 30 is

$$\mathcal{C}(18, 30) = \{-1, 1, -2, 2, -3, 3, -6, 6\}.$$

So, $\gcd(18, 30) = 6$.

4.4 Lemma $\gcd(a, b) = \gcd(b, a)$.

PROOF. Clearly the two sets $\mathcal{C}(a, b)$ and $\mathcal{C}(b, a)$ are equal. It follows that their largest elements are equal, that is, that $\gcd(a, b) = \gcd(b, a)$. QED

4.5 Lemma $\gcd(a, b) = \gcd(|a|, |b|)$.

PROOF. If $a = 0$ and $b = 0$ then $|a| = a$ and $|b| = b$, and so in this case $\gcd(a, b) = \gcd(|a|, |b|)$. Suppose that one of a or b is not 0. Lemma 1.4 shows that $d \mid a \Leftrightarrow d \mid |a|$. It follows that the two sets $\mathcal{C}(a, b)$ and $\mathcal{C}(|a|, |b|)$ are the same set. So the largest member of that set, the greatest common divisor of a and b, is also the greatest common divisor of $|a|$ and $|b|$. QED

4.6 Lemma If $a \neq 0$ or $b \neq 0$, then $\gcd(a, b)$ exists and satisfies

$$0 < \gcd(a, b) \leq \min\{|a|, |b|\}.$$

PROOF. Note that $\gcd(a,b)$ is the largest integer in the set $\mathcal{C}(a,b)$. Since $1 \mid a$ and $1 \mid b$ we know that $1 \in \mathcal{C}(a,b)$. So the greatest common divisor must be at least 1, and is therefore positive. On the other hand, if $d \in \mathcal{C}(a,b)$ then $d \mid |a|$ and $d \mid |b|$, so d is no larger than $|a|$ and no larger than $|b|$. Thus, d is at most the minimum of $|a|$ and $|b|$. QED

4.7 Example The above results give that

$$\gcd(48,732) = \gcd(-48,732) = \gcd(-48,-732) = \gcd(48,-732).$$

We also know that $0 < \gcd(48,732) \leq 48$. Since if $d = \gcd(48,732)$ then $d \mid 48$, to find d we need check only for positive divisors of 48 that also divide 732.

4.8 Remark Observe that the first two lemmas, which draw conclusions about the properties of the gcd operator, preceed Lemma 4.6, which shows that the gcd exists.

If two numbers have a greatest common divisor of 1 then they have no nontivial common factors.

4.9 Definition Two numbers are *relatively prime* if they have a greatest common divisor of 1.

Although the relatively prime relationship is symmetric — if $\gcd(a,b) = 1$ then $\gcd(b,a) = 1$ — we sometimes state it as "a is relatively prime to b."

4.10 Lemma If $g = \gcd(a,b)$ then $\gcd(a/g, b/g) = 1$.

PROOF. The greatest common divisor of a/g and b/g must exist, by the prior result. Let $\gcd(a/g, b/g) = k$. Then k is a divisor of both a/g and b/g so there are numbers j_a and j_b such that $j_a k = a/g$ and $j_b k = b/g$. Therefore $j_a(kg) = a$ and $j_b(kg) = b$, and so kg is a common divisor of a and b. If $k > 1$ this would be a contradiction, because then $kg > g$ but g is the greatest common divisor. Therefore $k = 1$. QED

Chapter 5

Bezout's Lemma

5.1 Definition A number c is a *linear combination* of the numbers a and b if $c = as + bt$ for some s and t.

5.2 Example The number $c = 16$ is a linear combination of $a = 2$ and $b = 5$ since taking $s = 3$ and $t = 2$ gives $16 = 3 \cdot 2 + 2 \cdot 5$. The number 21 is not a linear combination of 2 and 4, since in the equation $21 = s \cdot 2 + t \cdot 4$ the right side is divisible by 2 while the left is not. (That is, there are no integers s and t; we can solve the equation with rational numbers that are not integral.)

Thus, the Linearity statement in the Divisibility Properties theorem says that if d divides a and b, then d divides all linear combinations of a and b. So the greatest common divisor, $\gcd(a, b)$, divides every member of $\mathcal{L}(a, b)$, the set of all linear combinations of a and b. The next result says that $\gcd(a, b)$ is itself a member of $\mathcal{L}(a, b)$.

5.3 Lemma (Bezout's Lemma) The greatest common divisor of two numbers is a linear combination of those two: for all integers a and b there exist integers s and t such that $\gcd(a, b) = sa + tb$.

PROOF. If a and b are 0 then s and t may be anything since $\gcd(0, 0) = 0 = s \cdot 0 + t \cdot 0$. So we may assume that $a \neq 0$ or $b \neq 0$. Consider the set $\mathcal{L}(a, b) = \{na + mb : n, m \in \mathbb{Z}\}$ of all linear combinations of a and b.

Denote the set of positive members of $\mathcal{L}(a, b)$ by $\mathcal{L}^+(a, b)$. Note that $\mathcal{L}(a, b)$ contains a, $-a$, b and $-b$, and since $a \neq 0$ or $b \neq 0$, at least one of these four numbers is positive. Therefore $\mathcal{L}^+(a, b)$ is not empty. Because of this, by the Well-Ordering Property for $\mathbb{N}$, we know that the set $\mathcal{L}^+(a, b)$ contains a smallest positive integer; call it d. We will show that d is the greatest common divisor of a and b. That will finish the argument because d is a linear combination of a and b as it is a member of $\mathcal{L}$.

Since $d \in \mathcal{L}^+(a, b)$ we have $d = sa + tb$ for some integers s and t. Let $g = \gcd(a, b)$. Then $g \mid a$ and $g \mid b$, so by the Linearity property of Theorem 1.2, we have $g \mid (sa+tb)$, that is, $g \mid d$. Since g and d are positive, by the Comparision property of Theorem 1.2, we have that $g \leq d$.

If we show that d is a common divisor of a and b, then we will have that $d \leq g$ (as g is the greatest of the common divisors), and so we will have shown that $g = d$. To show that $d \mid a$, write $a = dq + r$ where $0 \leq r < d$ and compute

$$r = a - dq = a - (sa + tb)q = (1 - sq)a + (-tq)b.$$

to conclude that $r \in \mathcal{L}(a, b)$. Thus, if r were to be strictly greater than 0 then r would be a member of $\mathcal{L}^+(a, b)$. But this cannot be, since r is strictly less than d and d is the smallest integer in $\mathcal{L}^+(a, b)$. So we must have that $r = 0$. That is, $a = dq$, and hence $d \mid a$. A similar argument shows that $d \mid b$. Thus, d is indeed a common divisor of a and b, and $d = g = \gcd(a, b)$. QED

5.4 Example Notice that $1 = \gcd(2, 3)$ and $1 = (-1)2 + 1 \cdot 3$. Notice also that $1 = 2 \cdot 2 + (-1)3$. So the numbers s and t in Bezout's Lemma are uniquely determined. In fact, as we will see later that for each pair a, b there are infinitely many s and t.

5.5 Corollary The set $\mathcal{L}(a, b)$ of all linear combinations of a and b equals the set of multiples of $\gcd(a, b)$.

PROOF. We observed above that any member of $\mathcal{L}(a, b)$ is a multiple of $\gcd(a, b)$. For the converse, consider the multiple $k \cdot \gcd(a, b)$, apply Bezout's Lemma to get $s, t \in \mathbb{Z}$ so that $\gcd(a, b) = sa + tb$, and substitute: $k \cdot \gcd(a, b) = k \cdot (sa + tb) = (ks)a + (kt)b$. QED

5.6 Lemma If $a \mid bc$ and a is relatively prime to b then $a \mid c$.

PROOF. Since $\gcd(a, b) = 1$, by Bezout's Lemma there are coefficients s and t such that $1 = as+bt$. Multiply both sides by c to get $c = cas+cbt = a(cs)+(bc)t$. Note that $a \mid a(cs)$ and that $a \mid bc$ by assumption, so Theorem 1.2 gives that a divides the linear combination $a(cs) + (bc)t = c$. QED

Observe that $6 \mid (4 \cdot 9)$ but $6 \nmid 4$ and $6 \nmid 9$ (6 is not relatively prime to 4, and is also not relatively prime to 9). Thus the condition of relative primality is needed in that lemma.

We can completely characterize $\mathcal{L}(a, b)$.

5.7 Lemma Fix $a, b \in \mathbb{Z}$. If $\gcd(a, b) \mid c$ then the equation $sa + tb = c$ has infinitely many solution pairs s, t, which have the form

$$s = s_0 - j \cdot (b/d), \quad t = t_0 + j \cdot (a/d) \qquad j \in \mathbb{Z}$$

where s_0, t_0 is any particular solution pair.

PROOF. First assume that a solution pair s_0, t_0 exists, to show that any pair of numbers of that form also solve the equation. Plug them into the equation.

$$(s_0 - j(b/d)) \cdot a + (t_0 + j(a/d)) \cdot b = (s_0 a + t_0 b) + j(-(ab/d) + (ab/d)) = s_0 a + t_0 b = c$$

To finish we must show that pairs of the stated type are the only solutions.. Suppose that s and t also solve the equation: $sa + tb = c$. Subtracting gives $(s - s_0)a + (t - t_0)b = 0$, that is,

$$(*) \qquad (s - s_0)a = (t_0 - t)b.$$

Divide by $g = \gcd(a, b)$ on both sides to get $(s - s_0)(a/g) = (t_0 - t)(b/g)$, which shows that b/g divides $(s - s_0)(a/g)$. By Lemma 4.10, $\gcd(a/g, b/g) = 1$ and so the prior result, Lemma 5.6, shows that b/g divides $s - s_0$. Thus, for this solution pair s, t, there is a $j \in \mathbb{Z}$ such that $j \cdot (b/g) = s - s_0$, that is, s has the form $s = s_0 - j(b/g)$. With that form for s, substituting into equation $(*)$ gives that $((s_0 - j(b/g)) - s_0)a = -ja(b/g)$ equals $(t_0 - t)b$. Dividing both sides by b and rearranging gives that $t = t_0 + j(a/g)$. QED

Chapter 6

The Euclidean Algorithm

We can efficiently compute the greatest common divisor of two numbers.

We first reduce the problem. Since $\gcd(a, b) = \gcd(|a|, |b|)$ (and $\gcd(0, 0) = 0$), we need only give a method to compute $\gcd(a, b)$ where a and b are nonnegative. And, since $\gcd(a, b) = \gcd(b, a)$, it is enough for us to give a method for $a \geq b \geq 0$.

6.1 Lemma If $a > 0$ then $\gcd(a, 0) = a$.

PROOF. Since every integer divides 0, $\mathcal{C}(a, 0)$ is just the set of divisors of a. The largest divisor of a is $|a|$. Since a is positive, $|a| = a$, and so $\gcd(a, 0) = a$. QED

The prior lemma reduces the problem of computing $\gcd(a, b)$ to the case where $a \geq b > 0$.

6.2 Lemma If $a > 0$ then $\gcd(a, a) = a$.

PROOF. Obviously, a is a common divisor. By Lemma 4.6, $\gcd(a, a) \leq |a|$ and since a is positive, $|a| = a$. So a is the greatest common divisor. QED

We have now reduced the problem to the case $a > b > 0$. The central result is next.

6.3 Lemma Let $a > b > 0$. If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

PROOF. It suffices to show that the two sets $\mathcal{C}(a, b)$ and $\mathcal{C}(b, r)$ are equal, because then they must have the same greatest member. To show that the sets are equal we will show that they have the same members.

First, suppose that $d \in \mathcal{C}(a, b)$, so that $d \mid a$ and $d \mid b$. Note that $r = a - bq$. By Theorem 1.2(3) we have that $d \mid r$. Thus $d \mid b$ and $d \mid r$, and so $d \in \mathcal{C}(b, r)$. We have shown that any member of $\mathcal{C}(a, b)$ is a member of $\mathcal{C}(b, r)$, that is, that $\mathcal{C}(a, b) \subseteq \mathcal{C}(b, r)$.

For the other containment, assume that $d \in \mathcal{C}(b, r)$ so that $d \mid b$ and $d \mid r$. Since $a = bq + r$, Theorem 1.2(3) applies again to shows that $d \mid a$. So $d \mid a$ and $d \mid b$, and therefore $d \in \mathcal{C}(a, b)$. QED

The *Euclidean Algorithm* uses Lemma 6.3 to compute the greatest common divisor of two numbers. Rather introduce a computer language in which to give algorithm, we will illustrate it with an example.

6.4 Example Compute $\gcd(803, 154)$.

$$\begin{aligned}
\gcd(803, 154) &= \gcd(154, 33) && \text{since } 803 = 154 \cdot 5 + 33 \\
\gcd(154, 33) &= \gcd(33, 22) && \text{since } 154 = 33 \cdot 4 + 22 \\
\gcd(33, 22) &= \gcd(22, 11) && \text{since } 33 = 22 \cdot 1 + 11 \\
\gcd(22, 11) &= \gcd(11, 0) && \text{since } 22 = 11 \cdot 1 + 0 \\
\gcd(11, 0) &= 11
\end{aligned}$$

Hence $\gcd(803, 154) = 11$.

6.5 Remark This method is much faster than finding $\mathcal{C}(a, b)$ and can find gcd's of quite large numbers.

Recall that Bezout's Lemma asserts that given a and b there exists two numbers s and t such that $\gcd(a, b) = s \cdot a + t \cdot b$. We can use Euclid's Algorithm to find s and t by tracing through the steps, in reverse.

6.6 Example Express $\gcd(803, 154)$ as a linear combination of 803 and 154.

$$\begin{aligned}
11 &= 33 + 22 \cdot (-1) \\
&= 33 + (154 - 33 \cdot 4) \cdot (-1) = 154 \cdot (-1) + 33 \cdot 5 \\
&= 154 \cdot (-1) + (803 - 154 \cdot 5) \cdot 5 = 803 \cdot 5 + 154 \cdot (-26)
\end{aligned}$$

Chapter 7

The Fundamental Theorem

7.1 Theorem (Fundamental Theorem of Arithmetic) Every number greater than 1 factors into a product of primes $n = p_1 p_2 \cdots p_s$. Further, writing the primes in ascending order $p_1 \leq p_2 \leq \cdots \leq p_s$ makes the factorization unique.

Some of the primes in the product may be equal. For instance, $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$. So the Fundamental Theorem is sometimes stated as: every number greater than 1 can be factored uniquely as a product of powers of primes.

7.2 Example $600 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^3 \cdot 3 \cdot 5^2$

We will break the proof of the Fundamental Theorem into a sequence of Lemmas.

7.3 Lemma (Euclid's Lemma) If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

PROOF. Assume that $p \mid ab$. If $p \mid a$ then we are done, so suppose that it does not. Let $d = \gcd(p, a)$. Note that $d > 0$, and that $d \mid p$ and $d \mid a$. Since $d \mid p$ we have that $d = 1$ or $d = p$. If $d = p$ then $p \mid a$, which we assumed was not true. So we must have $d = 1$. Hence $\gcd(p, a) = 1$ and $p \mid ab$. So by Lemma 5.6, $p \mid b$. QED

7.4 Lemma Let p be prime. Let $a_1, a_2, \ldots, a_n$, $n \geq 1$, be integers. If $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for at least one $i \in \{1, 2, \ldots, n\}$.

PROOF. We use induction on n. For the $n = 1$ base case the result is clear.

For the inductive step, assume the inductive hypothesis: that the lemma holds for n such that $1 \leq n \leq k$. We must show that it holds for $n = k + 1$. Assume that p is prime and that $p \mid a_1 a_2 \cdots a_k a_{k+1}$. Write $a_1 a_2 \cdots a_k$ as a, and a_{k+1} as b. Then $p \mid a$ or $p \mid b$ by Lemma 7.3. If $p \mid a = a_1 \cdots a_k$ then by the induction hypothesis, $p \mid a_i$ for some $i \in \{1, \ldots, k\}$. If $p \mid b$ then $p \mid a_{k+1}$. So we can say that $p \mid a_i$ for some $i \in \{1, 2, \ldots, k+1\}$. This verifies the lemma for $n = k + 1$. Hence by mathematical induction, it holds for all $n \geq 1$. QED

7.5 Lemma (Fundamental Theorem, Existence) If $n > 1$ then there exist primes $p_1, \ldots, p_s$, where $s \geq 1$, such that $n = p_1 p_2 \cdots p_s$ and $p_1 \leq p_2 \leq \cdots \leq p_s$.

PROOF. We will use induction on n. The base step is $n = 2$: in this case, since 2 is prime we can take $s = 1$ and $p_1 = 2$.

For the inductive step, assume the hypothesis that the lemma holds for $2 \leq n \leq k$; we will show that it holds for $n = k + 1$. If $k + 1$ is prime then $s = 1$ and $p_1 = k + 1$. If $k + 1$ is composite then write $k + 1 = ab$ where $1 < a < k + 1$ and $1 < b < k + 1$. By the induction hypothesis there are primes $p_1, \ldots, p_u$ and $q_1, \ldots, q_v$ such that $a = p_1 \cdots p_u$ and $b = q_1 \cdots q_v$. This gives that $k + 1$ is a product of primes

$$k + 1 = ab = p_1 p_2 \cdots p_u q_1 q_2 \cdots q_v,$$

where $s = u + v$. Reorder the primes into ascending order, if necessary.

The base step and the inductive step together give us that the statement is true for all $n > 1$. QED

7.6 Lemma (Fundamental Theorem, Uniqueness) If $n = p_1 p_2 \cdots p_s$ for $s \geq 1$ with $p_1 \leq p_2 \leq \cdots \leq p_s$, and also $n = q_1 q_2 \cdots q_t$ for $t \geq 1$ with $q_1 \leq q_2 \leq \cdots \leq q_t$, then $t = s$, and $p_i = q_i$ for all i between 1 and s.

PROOF. The proof is by induction on s. In the $s = 1$ base case, $n = p_1$ is prime and we have $p_1 = q_1 q_2 \cdots q_t$. Now, t must be 1 or else this is a factorization of the prime p_1, and therefore $p_1 = q_1$.

Now assume the inductive hypothesis that the result holds for all s with $1 \leq s \leq k$. We must show that the result then holds for $s = k + 1$. Assume that $n = p_1 p_2 \cdots p_k p_{k+1}$ where $p_1 \leq p_2 \leq \cdots \leq p_{k+1}$, and also $n = q_1 q_2 \cdots q_t$ where $q_1 \leq q_2 \leq \cdots \leq q_t$. Clearly $p_{k+1} \mid n$, so $p_{k+1} \mid q_1 \cdots q_t$. Euclid's Lemma then gives that p_{k+1} divides some q_i. That implies that $p_{k+1} = q_i$, or else p_{k+1} would be a non-1 divisor of the prime q_i, which is impossible. Hence $p_{k+1} = q_i \leq q_t$.

A similar argument shows that $q_t = p_j \leq p_{k+1}$. Therefore $p_{k+1} = q_t$.

To finish, cancel $p_{k+1} = q_t$ from the two sides of this equation.

$$p_1 p_2 \cdots p_k p_{k+1} = q_1 q_2 \cdots q_{t-1} q_t$$

Now the induction hypothesis applies: $k = t - 1$ and $p_i = q_i$ for $i = 1, \ldots, t - 1$.

So the lemma holds also in the $s = k + 1$ case, and so by mathematical induction it holds for all $s \geq 1$. QED

7.7 Remark Unique factorization gives an alternative, conceptually simpler, way to find the greatest common divisor of two numbers. For example, $600 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^0$ and $252 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7$. Now, 2^3 divides both number. So does 3^1, but 3^2 does not divide both. Also, the highest power of 5 dividing both numbers is 5^0, and similarly the highest power of 7 that works for both is 7^0. So $\gcd(600, 252) = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 24$. In general, we can find the greatest common divisor of two numbers factoring, then taking the minimum power of 2, times the minimum power of 3, etc.

The difficulty with this method is that we must factor the numbers. But factorization is very difficult! That is, for numbers that are large, factoring is slow while the Euclidean algorithm is relatively fast.

Chapter 8

Distribution of Primes

The *Sieve of Eratosthenes* is an ancient method to find primes. To find the primes less than n, list the numbers from 2 to $n-1$. The smallest number, 2, is prime. Cross off all proper multiples of 2 (that is, the even numbers greater than 2). The smallest number remaining, 3, is prime. Cross off all proper multiples of 3, that is, 6, 9, etc. (some of them have already been eliminated). The smallest remaining number, 5, is prime. Cross off all proper multiples of 5. Continue this process until the list is exhausted.

Here is what is left when the sieve filters out the nonprimes less than 100.

	00	01	02	03	04	05	06	07	08	09
0			2	3		5		7		
10		11		13				17		19
20				23						29
30		31						37		
40		41		43				47		
50				53						59
60		61						67		
70		71		73						79
80				83						89
90								97		

Obviously, the columns with even numbers and the columns with multiples of 5 are empty (except for 2 and 5) but this is an artifact of the fact that the rows of the table are $10 = 2 \cdot 5$ wide. Other than that, at first glance no pattern is apparent.

8.1 Theorem (Wilson's Theorem) There are arbitrarily long gaps between primes: for any positive integer n there is a sequence of n consecutive composite integers.

PROOF. Given $n \geq 1$, consider $a = (n+1)! + 2$. We will show that all of the numbers $a, a+1, \ldots, a+(n-1)$ are composite.

Since $n+1 \geq 2$, clearly $2 \mid (n+1)!$. Hence $2 \mid (n+1)!+2$. Since $(n+1)!+2 > 2$, we therefore have that $a = (n+1)! + 2$ is composite. We will finish by showing that the i-th number in the sequence, $a + i$ where $0 \leq i \leq n-1$, is composite. Because $2 \leq i + 2 \leq n + 1$, we have that $(i + 2) \mid (n + 1)!$. Hence $i + 2 \mid a + i = (n+1)!+(i+2)$. Because $a+i > i+2 > 1$, we have that $a+i$ is composite. QED

8.2 Definition For any positive real number x, the number of primes less than or equal to x is $\pi(x)$.

For example, $\pi(10) = 4$.

The next result was first conjectured in 1793 by by Gauss, on the basis of numerical evidence like that in the table above. It was, however, not proved until over 100 years later, by Hadamard and Vallée Poussin. The proof is beyond the scope of this course.

8.3 Theorem (The Prime Number Theorem)

$$\lim_{x \to \infty} \frac{\pi(x)}{(x/\ln(x))} = 1.$$

Here is a table of values of $\pi(10^i)$ and $10^i/\ln(10^i)$ for $i = 2, \ldots, 10$ (the second set of values have been rounded to the nearest integer).

x	$\pi(x)$	round$(x/\ln(x))$
10^2	25	22
10^3	168	145
10^4	1229	1086
10^5	9592	8686
10^6	78498	72382
10^7	664579	620421
10^8	5761455	5428681
10^9	50847534	48254942
10^{10}	455052511	434294482

This table has been continued up to 10^{21}, but mathematicians are still working on finding the value of $\pi(10^{22})$. Of course, computing the approximations are easy, but finding the exact value of $\pi(10^{22})$ is hard.

Chapter 9

Fermat Primes and Mersenne Primes

A formula that produces the primes would be nice. Historically, lacking such a formula, mathematicians have looked for formulas that at least produce only primes.

In 1640 Fermat noted that the numbers in this list

n	0	1	2	3	4
$F_n = 2^{(2^n)} + 1$	3	5	17	257	65,537

are all prime. He conjectured that F_n is always prime. Numbers of the form $2^{2^n} + 1$ are called *Fermat numbers*.

9.1 Lemma Let $a > 1$ and $n > 1$. If $a^n + 1$ is prime then a is even and $n = 2^k$ for some $k \geq 1$.

PROOF. We first show that n is even. Suppose otherwise, and recall the well-known factorization.

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$$

Replace a by $-a$.

$$(-a)^n - 1 = (-a-1)\left((-a)^{n-1} + (-a)^{n-2} + \cdots + (-a) + 1\right)$$

If the exponent n is odd then $n-1$ is even, $n-2$ is odd, etc. So we have $(-a)^n = -a^n$, $(-a)^{n-1} = a^{n-1}$, $(-a)^{n-2} = -a^{n-2}$, etc., and the factorization becomes

$$-(a^n + 1) = -(a+1)\left(a^{n-1} - a^{n-2} + \cdots - a + 1\right).$$

Then changing the sign of both sides gives $(a^n + 1) = (a+1)(a^{n-1} - a^{n-2} + \cdots - a + 1)$. But with $n \geq 2$, we have $1 < a + 1 < a^n + 1$. This shows that if n is odd and $a > 1$, then $a^n + 1$ is not prime.

So n is even. Write $n = 2^s \cdot t$ where t is odd. Then if $a^n + 1$ is prime we have $(a^{2^s})^t + 1$ is prime. But by what we just showed this cannot be prime if t is odd and $t \geq 2$. So we must have $t = 1$ and therefore $n = 2^s$.

Also, $a^n + 1$ prime implies that a is even since if a is odd then so is a^n, and in consequence $a^n + 1$ would be even. But the only even prime is 2, adnd we are assuming that $a > 1$ and so we have $a \geq 2$, which implies that so $a^n + 1 \geq 3$. QED

9.2 Definition A prime number of the form $F_n = 2^{(2^n)} + 1$, $n \geq 0$, is a *Fermat prime*.

Euler showed that Fermat number next on the table, $F_5 = 4,294,967,297$, is composite.

As n increases, the F_n's increase in size very rapidly, and are not easy to check for primality. We know that F_n is composite for all n such that $5 \leq n \leq 30$, and a large number of other values of n including 382447 (the largest one that I know). Many researchers now conjecture that F_n is composite for $n \geq 5$. So Fermat's original thought that F_n is always prime is badly mistaken.

Mathematicians have also looked for formulas that produce many primes. That is, we can guess that numbers of various special forms are disproportionately prime. One form that has historically been of interest is are the *Mersenne numbers* $M_n = 2^n - 1$.

n	2	3	5	7	13
$f(n)$	3	7	31	127	8191

All of the numbers on the second row are prime. Note that $2^4 - 1$ is not prime, so this is not supposed to be a formula that gives only primes.

9.3 Lemma Let $a > 1$ and $n > 1$. If $a^n - 1$ is prime then $a = 2$ and n is prime.

PROOF. Consider again $a^n - 1 = (a-1)(a^{n-1} + \cdots + a + 1)$ Note that if $a > 2$ and $n > 1$ then $a - 1 > 1$ and $a^{n-1} + \cdots + a + 1 > a + 1 > 3$ so both factors are greater then 1, and therefore $a^n - 1$ is not prime. Hence if $a^n - 1$ is prime then we must have $a = 2$.

Now suppose $2^n - 1$ is prime. We claim that n is prime. For, if not, then $n = st$ where $1 < s < n$ and $1 < t < n$. Then $2^n - 1 = 2^{st} - 1 = (2^s)^t - 1$ is prime. But we just showed that if $a^n - 1$ is prime then we must have $a = 2$. So we must have $2^s = 2$, and hence $s = 1$ and $t = n$. Therefore n is not composite, that is, n is prime. QED

9.4 Corollary If M_n is prime, then n is prime.

PROOF. This is immediate from Lemma 9.3. QED

At first it was thought that $M_p = 2^p - 1$ is prime whenever p is prime. But in 1536, Hudalricus Regius showed that $M_{11} = 2^{11} - 1 = 2047$ is not prime: $2047 = 23 \cdot 89$.

9.5 Definition A prime number of the form $M_n = 2^n - 1$, $n \geq 2$, is a *Mersenne prime*.

People continue to work on determining which M_p's are prime. To date (2003-Dec-09), we know that $2^p - 1$ is prime if p is one of the following 40 primes: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, and 20996011.

The first number with more than a thousand digits known to be prime was M_{4253}. The largest number on that list was found on 2003-Nov-17. This number has $6,320,430$ digits. It was found as part of the Great Internet Mersenne Prime Search (GIMPS). (You can participate in this search by setting a program to run at times when your computer is not busy; see Chris Caldwell's page for more about this.) Later we will see a connection between Mersenne primes and perfect numbers.

One reason that we know so much about Mersenne primes is that the following test makes it easier to check whether or not M_p is prime when p is a large prime.

9.6 Theorem (The Lucas-Lehmer Mersenne Prime Test) Let p be an odd prime. Define the sequence $r_1, r_2, r_3, \ldots, r_{p-1}$ by the rules $r_1 = 4$, and for $k \geq 2$,

$$r_k = (r_{k-1}^2 - 2) \bmod M_p.$$

Then M_p is prime if and only if $r_{p-1} = 0$.

The proof of this is beyond the scope of this book.

9.7 Example Let $p = 5$. Then $M_p = M_5 = 31$.

$$\begin{aligned} r_1 &= 4 \\ r_2 &= (4^2 - 2) \bmod 31 = 14 \bmod 31 = 14 \\ r_3 &= (14^2 - 2) \bmod 31 = 194 \bmod 31 = 8 \\ r_4 &= (8^2 - 2) \bmod 31 = 62 \bmod 31 = 0 \end{aligned}$$

Hence by the Lucas-Lehmer test, $M_5 = 31$ is prime.

9.8 Remark Note that the Lucas-Lehmer test for $M_p = 2^p - 1$ takes only $p - 1$ steps. On the other hand, if we try to prove that M_p is prime by testing all primes less than or equal to $\sqrt{M_p}$ then must consider about $2^{(p/2)}$ steps. This is much larger, in general, than p.

No one knows whether there are infinitely many Mersenne primes.

Chapter 10

The Functions σ and τ

10.1 Definition Where n is a positive integer, $\tau(n)$ is the number of positive divisors of n.

10.2 Example The number $12 = 3 \cdot 2^2$ has positive divisors $1, 2, 3, 4, 6, 12$, and so $\tau(12) = 6$.

10.3 Definition Where n is a positive integer, $\sigma(n)$ is the sum of the positive divisors of n.

A positive divisor d of n is a *proper divisor* if $d < n$. The sum of all proper divisors of n is $\sigma^*(n)$.

Note that if $n \geq 2$ then $\sigma^*(n) = \sigma(n) - n$.

10.4 Example $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$, $\sigma^*(12) = 16$.

10.5 Definition A number $n > 1$ is *perfect* if $\sigma^*(n) = n$.

10.6 Example The first perfect number is 6 because its proper divisors are 1, 2 and 3.

10.7 Theorem Consider the prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$.

(1) $\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$

(2) $\sigma(n) = \dfrac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \dfrac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{e_r+1} - 1}{p_r - 1}$

10.8 Example If $n = 72 = 2^3 \cdot 3^2$ then $\tau(72) = (3 + 1)(2 + 1) = 12$ and

$$\sigma(72) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} = 15 \cdot 13 = 195.$$

Proof of item (1). From the Fundamental Theorem of Arithmetic, if d is a factor of n then the prime factors of d come from those of n. Hence $d \mid n$ iff $d = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ where for each i, $0 \leq f_i \leq e_i$. There are $(e_1+1)(e_2+1) \cdots (e_r+1)$ choices for the exponents $f_1, f_2, \ldots, f_r$. QED

Our proof of the second item requires two preliminary results.

10.9 Lemma Suppose that $n = ab$, where $a > 0$, $b > 0$ and $\gcd(a, b) = 1$. Then $\sigma(n) = \sigma(a)\sigma(b)$.

PROOF. Since a and b have only 1 as a common factor, the Fundamental Theorem of Arithmetic, shows that $d \mid n$ only when d factors into $d = d_1 d_2$ where $d_1 \mid a$ and $d_2 \mid b$. That is, the divisors of ab are products of the divisors of a with the divisors of b. Let the divisors of a be $1, a_1, \ldots, a_s$ and the divisors of b be $1, b_1, \ldots, b_t$. These are the divisors of $n = ab$.

$$\begin{gathered} 1, b_1, b_2, \ldots, b_t \\ a_1 \cdot 1, a_1 \cdot b_1, a_1 \cdot b_2, \ldots, a_1 \cdot b_t \\ a_2 \cdot 1, a_2 \cdot b_1, a_2 \cdot b_2, \ldots, a_2 \cdot b_t \\ \vdots \\ a_s \cdot 1, a_s \cdot b_1, a_s \cdot b_2, \ldots, a_s \cdot b_t \end{gathered}$$

This list has no repetitions because, as $\gcd(a, b) = 1$, if $a_i b_j = a_k b_\ell$ then $a_i = a_k$ and $b_j = b_\ell$. Therefore to find $\sigma(b)$ we can sum the rows

$$\begin{aligned} 1 + b_1 + \cdots + b_t &= \sigma(b) \\ a_1 1 + a_1 b_1 + \cdots + a_1 b_t &= a_1 \sigma(b) \\ &\vdots \\ a_s \cdot 1 + a_s b_1 + \cdots + a_s b_t &= a_s \sigma(b) \end{aligned}$$

and add those partial sums

$$\begin{aligned} \sigma(n) &= \sigma(b) + a_1\sigma(b) + a_2\sigma(b) + \cdots + a_3\sigma(b) \\ &= (1 + a_1 + a_2 + \cdots + a_s)\sigma(b) \\ &= \sigma(a)\sigma(b) \end{aligned}$$

to get the required result. QED

10.10 Lemma If p is a prime and $k \geq 0$ then

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

PROOF. Since p is prime, the divisors of p^k are $1, p, p^2, \ldots, p^k$. Hence

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}$$

follows from the formula for the sum of a geometric series. QED

Proof of item (2). Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. This proof is by induction on the number of prime factors r. In the $r = 1$ base case we have $n = p_1^{e_1}$ and the result follows from Lemma 10.10.

For the inductive step, the inductive hypothesis is that the statment is true when $1 \leq r \leq k$. Consider the $r = k + 1$ case: $n = p_1^{e_1} \cdots p_k^{e_k} p_{k+1}^{e_{k+1}}$ where the primes are distinct. Let $a = p_1^{e_1} \cdots p_k^{e_k}$ and $b = p_{k+1}^{e_{k+1}}$. Clearly $\gcd(a, b) = 1$. Lemma 10.9 applies to give that $\sigma(n) = \sigma(a)\sigma(b)$. The inductive hypothesis and Lemma 10.10 give

$$\sigma(a) = \left(\frac{p_1^{e_1+1} - 1}{p_1 - 1}\right) \cdots \left(\frac{p_k^{e_k+1} - 1}{p_k - 1}\right) \qquad \sigma(b) = \frac{p_{k+1}^{e_{k+1}+1} - 1}{p_{k+1} - 1}$$

and therefore

$$\sigma(n) = \left(\frac{p_1^{e_1+1} - 1}{p_1 - 1}\right) \cdots \left(\frac{p_{k+1}^{e_{k+1}+1} - 1}{p_{k+1} - 1}\right)$$

as desired. So the result holds for $r = k + 1$, and that implies that the theorem is true for all integers by the principle of mathematical induction. QED

Chapter 11

Perfect Numbers and Mersenne Primes

A search for perfect numbers up to $10,000$ finds only these.

$$6 = 2 \cdot 3$$
$$28 = 2^2 \cdot 7$$
$$496 = 2^4 \cdot 31$$
$$8128 = 2^6 \cdot 127$$

Note that $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1$, and $127 = 2^7 - 1$ are Mersenne primes. We can conjecture that all perfect numbers fit this pattern. This chapter discusses to what extent this is known to be true.

11.1 Theorem If $2^p - 1$ is a Mersenne prime then $2^{p-1} \cdot (2^p - 1)$ is perfect.

PROOF. Write $q = 2^p - 1$ and $n = 2^{p-1}q$. Since q is odd and prime, Theorem 10.7 gives that $\sigma(n)$ is

$$\sigma\left(2^{p-1}q\right) = \left(\frac{2^p - 1}{2 - 1}\right)\left(\frac{q^2 - 1}{q - 1}\right) = (2^p - 1)(q + 1) = (2^p - 1)2^p = 2n.$$

That is, $\sigma(n) = 2n$, and so n is perfect. QED

11.2 Theorem If n is even and perfect then there is a Mersenne prime $2^p - 1$ such that $n = 2^{p-1}(2^p - 1)$.

PROOF. Suppose that n is even and perfect. Factor out all of the 2's to get $n = 2^k \cdot q$ with q an odd number, and $k \geq 1$ since n is even. Since q is odd, $\gcd(2^k, q) = 1$ and so by Lemmas 10.9 and 10.10 we have $\sigma(n) = \sigma(2^k)\sigma(q) = (2^{k+1} - 1)\sigma(q)$. Thus, as n is perfect,

$$2^{k+1}q = 2n = \sigma(n) = (2^{k+1} - 1)\sigma(q).$$

Now substituting $\sigma(q) = \sigma^*(q) + q$, into the prior displayed equation gives

$$2^{k+1}q = (2^{k+1} - 1)(\sigma^*(q) + q)$$

that is

$$2^{k+1}q = (2^{k+1} - 1)\sigma^*(q) + 2^{k+1}q - q$$

This implies that

$$(*) \qquad \sigma^*(q)(2^{k+1} - 1) = q.$$

So $\sigma^*(q)$ is a divisor of q. Since $k \geq 1$ we have that $2^{k+1} - 1 \geq 4 - 1 = 3$. So $\sigma^*(q)$ is a proper divisor of q. But $\sigma^*(q)$ is the sum of all of the proper divisors of q. This can only happen if q has only one proper divisor, that is, it implies that q is prime and so $\sigma^*(q) = 1$. Then equation $(*)$ shows that $q = 2^{k+1} - 1$. So q is a Mersenne prime and $k + 1 = p$ is prime. Therefore $n = 2^{p-1} \cdot (2^p - 1)$, as desired. QED

11.3 Corollary There is a one-to-one correspondence between the even perfect numbers and the Mersenne primes.

Here are two questions that remain open: (i) Are there infinitely many even perfect numbers? (ii) Are there any odd perfect numbers? (We know that if an odd perfect number exists, then it must be greater than 10^{50}.)

Chapter 12

Congruences

12.1 Definition Let $m \geq 0$. We we say that the numbers a and b are *congruent modulo* m, denoted $a \equiv b \pmod{m}$, if a and b leave the same remainder when divided by m. The number m is the *modulus* of the congruence. The notation $a \not\equiv b \pmod{m}$ means that they are not congruent.

12.2 Lemma The numbers a and b are congruent modulo m if and only if $m \mid (a-b)$, and also if and only if $m \mid (b-a)$.

PROOF. Write $a = mq_a + r_a$ and $b = mq_b + r_b$ for some q_a, q_b, r_a, and r_b, with $0 \leq r_a, r_b < m$. Subtracting gives $a - b = m(q_a - q_b) + (r_a - r_b)$. Observe that the restrictions on the remainders imply that $-m < r_a - r_b < m$, and so $r_a - r_b$ is not a multiple of m unless $r_a - r_b = 0$.

If a and b are congruent modulo m then $r_a = r_b$, which implies that $a - b = m(q_a - q_b)$, which in turn gives that $a - b$ is a multiple of m.

The implications in the prior paragraph reverse: if $a - b$ is a multiple of m then in the equation $a - b = m(q_a - q_b) + (r_a - r_b)$ we must have that $r_a - r_b = 0$ by the observation in the first paragraph, and therefore $r_a = r_b$.

The $b - a$ statement is proved similarly. QED

12.3 Examples

1. $25 \equiv 1 \pmod{4}$ since $4 \mid 24$
2. $25 \not\equiv 2 \pmod{4}$ since $4 \nmid 23$
3. $1 \equiv -3 \pmod{4}$ since $4 \mid 4$
4. $a \equiv b \pmod{1}$ for all a, b
5. $a \equiv b \pmod{0} \iff a = b$ for all a, b

Do not confuse the use of mod in Definition 12.1

$$a \equiv b \pmod{m} \text{ if } m \mid a - b$$

with that of Definition 3.3.

$$a \bmod b = r \text{ where } r \text{ is the remainder when } a \text{ is divided by } b$$

The two are related but not identitical.

12.4 Example One difference between the two is that $25 \equiv 5 \pmod 4$ is true while $25 = 5 \bmod 4$ is false (it asserts that $25 = 1$).

The 'mod' in $a \equiv b \pmod m$ defines a binary relation, a relationship between two things. The 'mod' in $a \bmod b$ is a binary operation, just as addition or multiplication are binary operations. Thus,

$$a \equiv b \pmod m \iff a \bmod m = b \bmod m.$$

That is, if $m > 0$ and $a \equiv r \pmod m$ where $0 \leq r < m$ then $a \bmod m = r$.

Expressions such as

$$x = 2$$
$$4^2 = 16$$
$$x^2 + 2x = \sin(x) + 3$$

are equations. By analogy, expressions such as

$$x \equiv 2 \pmod{16}$$
$$25 \equiv 5 \pmod 5$$
$$x^3 + 2x \equiv 6x^2 + 3 \pmod{27}$$

are called *congruences*.

The next two theorems show that congruences and equations share many properties.

12.5 Theorem Congruence is an equivalence relation: for all a, b, c, and $m > 0$ we have

(1) *(Reflexivity property)* $a \equiv a \pmod m$
(2) *(Symmetry property)* $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$
(3) *(Transitivity property)* $a \equiv b \pmod m$ and $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

PROOF. For reflexivity: on division by m, any number leaves the same remainder as itself.

For symmetry, if a leaves the same remainder as b, then b leaves the same remainder as a.

For transitivity, assume that a leaves the same remainder as b on division by m, and that b leaves the same remainder as c. The all three leave the same remainder as each other, and in particular a leaves the same remainder as c. QED

Below we will consider polynomials $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. We will assume that the coefficients $a_n, \ldots, a_0$ are integers and that x also represents an integer variable. Here the degree of the polynomial is an integer $n \geq 0$.

12.6 Theorem If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
(1) $a + c \equiv b + d \pmod{m}$ and $a - c \equiv b - d \pmod{m}$
(2) $ac \equiv bd \pmod{m}$
(3) $a^n \equiv b^n \pmod{m}$ for all $n \geq 1$
(4) $f(a) \equiv f(b) \pmod{m}$ for all polynomials $f(x)$ with integer coefficients.

Proof of (1). Since $a - c = a + (-c)$, it suffices to prove only the addition case. By assumption $m \mid a - b$ and $m \mid c - d$. By linearity of the 'divides' relation, $m \mid (a - b) + (c - d)$, that is $m \mid (a + c) - (b + d)$. Hence $a + c \equiv b + d \pmod{m}$. QED

Proof of (2). Since $m \mid a - b$ and $m \mid c - d$, by linearity $m \mid c(a - b) + b(c - d)$. Now, $c(a - b) + b(c - d) = ca - bd$, hence $m \mid ca - bd$, and so $ca \equiv bd \pmod{m}$, as desired. QED

Proof of (3). We prove this by induction on n. If $n = 1$, the result is true by the assumption that $a \equiv b \pmod{m}$. Assume that the result holds for $n = 1, \ldots, k$. Then we have $a^k \equiv b^k \pmod{m}$. This, together with $a \equiv b \pmod{m}$ using property (2) above, gives that $aa^k \equiv bb^k \pmod{m}$. Hence $a^{k+1} \equiv b^{k+1} \pmod{m}$ and the result holds in the $n = k + 1$ case. So the result holds for all $n \geq 1$, by induction. QED

Proof of (4). Let $f(x) = c_n x^n + \cdots + c_1 x + c_0$. We prove by induction on the degree of the polynomial n that if $a \equiv b \pmod{m}$ then $c_n a^n + \cdots + c_0 \equiv c_n b^n + \cdots + c_0 \pmod{m}$. For the degree $n = 0$ base case, by the reflexivity of congruence we have that $c_0 \equiv c_0 \pmod{m}$.

For the induction assume that the result holds for $n = k$. Then we have

$$(*) \qquad c_k a^k + \cdots + c_1 a + c_0 \equiv c_k b^k + \cdots + c_1 b + c_0 \pmod{m}.$$

By item (3) above we have $a^{k+1} \equiv b^{k+1} \pmod{m}$. Since $c_{k+1} \equiv c_{k+1} \pmod{m}$, using item (2) above we have

$$(**) \qquad c_{k+1} a^{k+1} \equiv c_{k+1} b^{k+1} \pmod{m}.$$

Now we can apply Theorem 15.3 (1) to $(*)$ and $(**)$ to obtain

$$c_{k+1} a^{k+1} + c_k a^k + \cdots + c_0 \equiv c_{k+1} b^{k+1} + c_k b^k + \cdots + c_0 \pmod{m}.$$

So by induction the result holds for all $n \geq 0$. QED

12.7 Example (From [1].) The first five Fermat numbers 3, 5, 17, 257, and $65,537$ are prime. We will use congruences to show that $F_5 = 2^{32} + 1$ is divisible by 641 and is therefore not prime.

Everyone knows that $2^2 = 4$, $2^4 = 16$, and $2^8 = 256$. Also, $2^{16} = (2^8)^2 = 256^2 = 65,536$. A straightforward division shows that $65,536 \equiv 154 \pmod{641}$.

Next, for 2^{32}, we have that $(2^{16})^2 \equiv (154)^2 \pmod{641}$. That is, $2^{32} \equiv 23,716 \pmod{641}$. Since an easy division finds that $23,716 \equiv 640 \pmod{641}$, and $640 \equiv -1 \pmod{641}$, we have that $2^{32} \equiv -1 \pmod{641}$. Hence $2^{32}+1 \equiv 0 \pmod{641}$, and so . $641 \mid 2^{32}+1$, as claimed. Clearly $2^{32}+1 \neq 641$, so $2^{32}+1$ is composite.

The work done here did not require us to find the value of $2^{32} + 1 = 4,294,967,297$ and divide it by 641; instead the calculations were with much smaller numbers.

Chapter 13

Divisibility Tests

Elementary school children know how to tell if a number is even, or divisible by 5, by looking at the least significant digit.

13.1 Theorem If a number a has the decimal representation $a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0$ then

(1) $a \bmod 2 = a_0 \bmod 2$

(2) $a \bmod 5 = a_0 \bmod 5$

PROOF. Consider $f(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Note that $10 \equiv 0 \pmod 2$. So by Theorem 12.6

$$a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \equiv a_{n-1}0^{n-1} + \cdots + a_1 0 + a_0 \pmod 2.$$

That is, $a \equiv a_0 \pmod 2$; this proves item (1). Since $10 \equiv 0 \pmod 5$ also, the proof of item (2) is similar. QED

13.2 Example Thus, the number 1457 is odd because 7 is odd: $1457 \bmod 2 = 7 \bmod 2 = 1$. And on division by 5 it leaves a remainder of $1457 \bmod 5 = 7 \bmod 5 = 2$.

13.3 Theorem Where $a = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0$ is the decimal representation,

(1) $a \bmod 3 = (a_{n-1} + \cdots + a_0) \bmod 3$

(2) $a \bmod 9 = (a_{n-1} + \cdots + a_0) \bmod 9$

(3) $a \bmod 11 = (a_0 - a_1 + a_2 - a_3 + \cdots) \bmod 11$.

PROOF. Note that $10 \equiv 1 \pmod 3$. Theorem 12.6 gives

$$a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \equiv a_{n-1}1^{n-1} + \cdots + a_1 1 + a_0 \pmod 3$$

and so $a \equiv a_{n-1} + \cdots + a_1 + a_0 \pmod 3$. This proves item (1). Since $10 \equiv 1 \pmod 9$ also, the proof of item (2) is similar.

For item (3), note that $10 \equiv -1 \pmod{11}$ so

$$a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \equiv a_{n-1}(-1)^{n-1} + \cdots + a_1(-1) + a_0 \pmod{11}.$$

That is, $a \equiv a_0 - a_1 + a_2 - \cdots \pmod{11}$. QED

13.4 Example Consider 1457 again. For divisibility by 3 we have $1457 \bmod 3 = (1+4+5+7) \bmod 3 = 17 \bmod 3 = 8 \bmod 3 = 2$. As for 9, we get $1457 \bmod 9 = (1+4+5+7) \bmod 9 = 17 \bmod 9 = 8 \bmod 9 = 8$. Finally, for 11, the calculation is $1457 \bmod 11 = 7 - 5 + 4 - 1 \bmod 11 = 5 \bmod 11 = 5$.

Note that $m \mid a \Leftrightarrow a \bmod m = 0$ so from the prior two results we obtain immediately the following.

13.5 Corollary Let $a = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0$.
(1) $2 \mid a \Leftrightarrow a_0 = 0, 2, 4, 6$ or 8
(2) $5 \mid a \Leftrightarrow a_0 = 0$ or 5
(3) $3 \mid a \Leftrightarrow 3 \mid a_0 + a_1 + \cdots + a_{n-1}$
(4) $9 \mid a \Leftrightarrow 9 \mid a_0 + a_1 + \cdots + a_{n-1}$
(5) $11 \mid a \Leftrightarrow 11 \mid a_0 - a_1 + a_2 - a_3 + \cdots$.

13.6 Theorem Let $a = a_r 10^r + \cdots + a_2 10^2 + a_1 10 + a_0$ be the decimal representation, so that we write a as the sequence $a_r a_{r-1} \cdots a_1 a_0$. Then
(1) $7 \mid a \Leftrightarrow 7 \mid a_r \cdots a_1 - 2a_0$.
(2) $13 \mid a \Leftrightarrow 13 \mid a_r \cdots a_1 - 9a_0$
(where $a_r \cdots a_1$ is the sequence representing $(a - a_0)/10$).

PROOF. For item (1), let $c = a_r \cdots a_1$ so that $a = 10c + a_0$. Since $\gcd(7, -2) = 1$ we have that $7 \mid a \Leftrightarrow 7 \mid -2a$. Consequently, consider $-2a = -20c - 2a_0$. Because $1 \equiv -20 \pmod{7}$, we have that $-2a \equiv c - 2a_0 \pmod{7}$. Therefore, $7 \mid -2a \Leftrightarrow 7 \mid c - 2a_0$. It follows that $7 \mid a \Leftrightarrow 7 \mid c - 2a_0$, which is what we wanted to prove.

The proof of item (2) is similar. QED

13.7 Example We can test whether 7 divides 2481.

$$7 \mid 2481 \Leftrightarrow 7 \mid 248 - 2 \Leftrightarrow 7 \mid 246 \Leftrightarrow 7 \mid 24 - 12 \Leftrightarrow 7 \mid 12$$

Since $7 \nmid 12$ we have that $7 \nmid 2481$.

13.8 Example The number 12987 is divisible by 13 because

$$13 \mid 12987 \Leftrightarrow 13 \mid 1298 - 63 \Leftrightarrow 13 \mid 1235 \Leftrightarrow 13 \mid 123 - 45 \Leftrightarrow 13 \mid 78$$

and $13 \cdot 6 = 78$.

Chapter 14

More Properties of Congruences

Theorem 12.6 provides some laws of algebra for $\equiv$. A typical algebra problem is to solve for an unknown; for instance, we can look for x such that $2x \equiv 7 \bmod 15$.

14.1 Theorem Let $m \geq 2$. If a and m are relatively prime then there exists a unique integer a^* such that $aa^* \equiv 1 \pmod{m}$ and $0 < a^* < m$.

PROOF. Assume that $\gcd(a, m) = 1$. Bezout's Lemma applies to give an s and t such that $as + mt = 1$. Hence $as - 1 = m(-t)$, that is, $m \mid as - 1$ and so $as \equiv 1 \pmod{m}$. Accordingly, let $a^* = s \bmod m$ so that $0 < a^* < m$. Then $a^* \equiv s \pmod{m}$ so $aa^* \equiv 1 \pmod{m}$.

To show uniqueness, assume that $ac \equiv 1 \pmod{m}$ and $0 < c < m$. Then $ac \equiv aa^* \pmod{m}$. Multiply both sides of this congruence on the left by c and use the fact that $ca \equiv 1 \pmod{m}$ to obtain $c \equiv a^* \pmod{m}$. Because both are in $[0\,..\,m)$, it follows that $c = a^*$. QED

We call a^* the *inverse* of a modulo m. Note that we do not denote a^* by a^{-1} here since we keep that symbol for the usual meaning of inverse.

14.2 Remark The proof shows that Blankinship's Method will compute the inverse of a, when it exists. But for small m we may find a^* by trial and error. For example, take $m = 15$ and $a = 2$. We can check each possibility: $2 \cdot 0 \not\equiv 1 \pmod{15}$, $2 \cdot 1 \not\equiv 1 \pmod{15}$, ..., $2 \cdot 8 \equiv 1 \pmod{15}$. So we can take $2^* = 8$.

Note that we may well have $ca \equiv 1 \bmod m$ with $c \neq a$ if $c \equiv a^* \pmod{m}$ and $c > m$ or $c < 0$. For instance, $8 \cdot 2 \equiv 1 \bmod 15$ and also $23 \cdot 2 \equiv 1 \bmod 15$. So the inverse is unique only if we specify that $0 < a^* < m$.

The converse of Theorem 14.1 holds.

14.3 Theorem Let $m > 0$. If $ab \equiv 1 \pmod{m}$ then both a and b are relatively prime to m.

PROOF. If $ab \equiv 1 \pmod{m}$, then $m \mid ab-1$. So $ab-1 = mt$ for some t. Hence, $ab + m(-t) = 1$.

The proof of Bezout's Lemma, Lemma 5.3, shows that $\gcd(a, m)$ is the smallest positive linear combination of a and m. The last paragraph shows that there is a combination that adds to 1. Since no combination can be positive and smaller than 1, we have that $\gcd(a, m) = 1$. The case of $\gcd(b, m)$ is similar.. QED

14.4 Corollary A number a has an inverse modulo m if and only if a and m are relatively prime.

The second paragraph of Theorem 14.1 uses a technique that is worth isolating.

14.5 Theorem (Cancellation) Let $m > 0$. If $\gcd(c, m) = 1$ then $ca \equiv cb \pmod{m} \Rightarrow a \equiv b \pmod{m}$.

PROOF. If $\gcd(c, m) = 1$ then it has an inverse c^* modulo m, such that $c^*c \equiv 1 \pmod{m}$. Since $ca \equiv cb \pmod{m}$ by Theorem 12.6, $c^*ca \equiv c^*cb \pmod{m}$. But $c^*c \equiv 1 \pmod{m}$ so $c^*ca \equiv a \pmod{m}$ and $c^*cb \equiv b \pmod{m}$. By reflexivity and transitivity this yields $a \equiv b \pmod{m}$. QED

Although in general we cannot cancel if $\gcd(c, m) > 1$, the next result is some consolation.

14.6 Theorem If $c > 0$ and $m > 0$ then $a \equiv b \pmod{m} \Leftrightarrow ca \equiv cb \pmod{cm}$.

PROOF. The congruence $a \equiv b \pmod{m}$ is true if and only if $m \mid (a-b)$ holds, which in turn holds if and only if $cm \mid (ca - cb)$. QED

14.7 Theorem Fix $m > 0$ and let $d = \gcd(c, m)$. Then $ca \equiv cb \pmod{m} \Rightarrow a \equiv b \pmod{m/d}$.

PROOF. Since $d = \gcd(c, m)$, the equations $c = d(c/d)$ and $m = d(m/d)$ involve integers. Rewriting $ca \equiv cb \pmod{m}$ gives

$$d\left(\frac{c}{d}\right) a \equiv d\left(\frac{c}{d}\right) b \pmod{d\left(\frac{m}{d}\right)}.$$

By Theorem 14.6 we have

$$\left(\frac{c}{d}\right) a \equiv \left(\frac{c}{d}\right) b \pmod{\frac{m}{d}}.$$

Since $d = \gcd(c, m)$, we have that $\gcd(c/d, m/d) = 1$ and so by cancellation, Theorem 14.5, $a \equiv b \pmod{m/d}$. QED

14.8 Theorem If $m > 0$ and $a \equiv b \pmod{m}$ then $\gcd(a, m) = \gcd(b, m)$.

PROOF. Let $d_a = \gcd(m, a)$ and $d_b = \gcd(m, b)$. Since $a \equiv b \pmod{m}$ we have $a - b = mt$ for some t. Rewrite that as $a = mt + b$ and note that $d_b \mid m$ and $d_b \mid b$, so $d_b \mid a$. Thus, d_b is a common divisor of m and a, and so $d_b \leq d_a$. A similar argument gives that $d_a \leq d_b$, and therefore $d_b = d_a$. QED

14.9 Corollary Fix $m > 0$. If $a \equiv b \pmod{m}$ then a has an inverse modulo m if and only if b does also.

PROOF. Immediate. QED

Chapter 15

Residue Classes

The work that we've seen shows that if $a \equiv b \pmod{m}$ then the two numbers a and b, while not necessarily equal, are in some ways alike.

15.1 Definition Fix $m > 0$. The *residue class* class of a modulo m (or *congruence class*, or *equivalence class of a modulo m*) is $[a] = \{x \mid x \equiv a \pmod{m}\}$, the set of all integers congruent to a modulo m.

Note that, by definition, $[a]$ is a set.

$$[a] = \{mq + a \mid q \in \mathbb{Z}\} = \{\dots, -2m + a, -m + a, a, m + a, 2m + a, \dots\}$$

Note also that $[a]$ depends on m and so it would be more accurate to write $[a]_m$ instead, but this would be cumbersome.

15.2 Theorem If $m > 0$ then $[a] = [b] \Leftrightarrow a \equiv b \pmod{m}$.

PROOF. First assume that $[a] = [b]$. Note that $a \in [a]$ because $a \equiv a \pmod{m}$. And, because $[a] = [b]$, we have $a \in [b]$. By definition of $[b]$, then $a \equiv b \pmod{m}$.

For the implication the other way, assume that $a \equiv b \pmod{m}$, aiming to prove that the sets $[a]$ and $[b]$ are equal. To prove that the sets are equal, we will prove that every element of the first is a member of the second, and vice versa. Suppose that $x \in [a]$, so that $x \equiv a \pmod{m}$. Since $a \equiv b \pmod{m}$, by transitivity of equivalence, $x \equiv b \pmod{m}$, and so $x \in [b]$. The argument to show that if $x \in [b]$ then $x \in [a]$ is similar. QED

15.3 Theorem Given $m > 0$. For every a there is a unique $r \in [0\,..\,m)$ such that $[a] = [r]$.

PROOF. Let $r = a \bmod m$ so that $0 \leq r < m$, and $a \equiv r \pmod{m}$, and by Theorem 15.2, $[a] = [r]$. To prove that r is unique, suppose that $[a] = [r']$, where $0 \leq r' < m$. By Theorem 15.2, this implies that $a \equiv r' \pmod{m}$. This, together with the restriction that $0 \leq r' < m$, implies that $r' = a \bmod m = r$. QED

15.4 Theorem Given $m > 0$, there are exactly m distinct residue classes modulo m, namely, [0], [1],..., and $[m - 1]$.

PROOF. By Theorem 15.3 we know that every residue class $[a]$ is equal to one of $[0]$, or $[1]$, ..., or $[m-1]$. So any residue classes is in this list. These residue classes are distinct: if $0 \leq r_1 < m$ and $0 \leq r_2 < m$ and $[r_1] = [r_2]$ then by the uniqueness part of Theorem 15.3 we must have $r_1 = r_2$. QED

15.5 Definition Any element $x \in [a]$ is a *class representative*. The element of $[a]$ that is in $[0\,..\,m)$ is the *principle class representative* or *principle residue*.

Chapter 16

$\mathbb{Z}_m$ and Complete Residue Systems

Throughout this section we assume a fixed modulus $m > 0$.

16.1 Definition The set $\{[a] \mid a \in \mathbb{Z}\}$ of all residue classes modulo m is denoted $\mathbb{Z}_m$.

Recall that in a set, the order in which elements appear does not matter, and repeat elements collapse: the set $\{0, 2, 3, 1\}$ and the set $\{2, 0, 2, 3, 1, 4, 1\}$ are equal. So, while at first glance $\mathbb{Z}_m$ may seem to have infinitely many elements $\mathbb{Z}_m = \{\dots, [-2], [-1], [0], [1], [2], \dots\}$, Theorem 15.4 shows that after the repeats collapse $\mathbb{Z}_m = \{[0], [1], \dots, [m-1]\}$, and so instead $\mathbb{Z}_m$ has exactly m elements.

16.2 Example Fix $m = 4$. Then $[1] = \{\dots, -7, -3, 1, 5, \dots\}$, and so all of these classes are equal: $\cdots = [-7] = [-3] = [1] = [5] = \cdots$. We could, therefore, instead of $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$, write $\mathbb{Z}_4 = \{[8], [5], [-6], [11]\}$.

16.3 Definition A set of m integers $\{a_0, a_1, \dots, a_{m-1}\}$ is a *complete residue system modulo m* (or a *complete set of representatives* for $\mathbb{Z}_m$) if the set $\mathbb{Z}_m$ equals the set $\{[a_0], [a_1], \dots, [a_{m-1}]\}$.

16.4 Example These are complete residue systems modulo 5.

1. $\{0, 1, 2, 3, 4\}$
2. $\{-2, -1, 0, 1, 2\}$
3. $\{-9, 14, 12, 10, 8\}$
4. $\{0 + 5n_1, 1 + 5n_2, 2 + 5n_3, 3 + 5n_4, 4 + 5n_4\}$, where n_1, n_2, n_3, n_4, n_5 may be any integers.

For each $m > 0$ there are infinitely many distinct complete residue systems modulo m. In particular, $\{0, 1, \dots, m-1\}$ is the set of *least nonnegative residues modulo m*.

16.5 Theorem Fix $m > 0$. If $m = 2k$ then $\{0, 1, 2, \ldots, k-1, k, -(k-1), \ldots, -2, -1\}$ is a complete residue system modulo m. If $m = 2k+1$, then $\{0, 1, 2, \ldots, k, -k, \ldots, -2, -1\}$ is a complete residue system modulo m.

PROOF. If $m = 2k$, then since $\mathbb{Z}_m = \{[0], [1], \ldots, [k], [k+1], \ldots, [k+i], [k+k-1]\}$, it suffices to note that $[k+i] = [k+i-2k] = [-k+i] = [-(k-i)]$. So $[k+1] = [-(k-1)], [k+2] = [-(k-2)], \ldots, [k+k-1] = [-1]$, as desired.

In the $n = 2k+1$ case, $[k+i] = [-(2k+1)+k+i] = [-k+i+1] = [-(k-i+1)]$ so $[k+1] = [-k], [k+2] = [-(k-1)], \ldots, [2k] = [-1]$, as desired. QED

16.6 Definition The complete residue system modulo m given in the prior theorem is the *least absolute residue system modulo m.*

16.7 Example Where $m = 2^{32}$, the least absolute residue system is

$$\{-(2^{31}-1), -(2^{31}-2), \ldots, -2, -1, 0, 1, 2, \ldots, 2^{31}\}.$$

Chapter 17

Addition and Multiplication in $\mathbb{Z}_m$

In this chapter we show how to define addition and multiplication of residue classes modulo m. With respect to these binary operations $\mathbb{Z}_m$ is a *ring* as defined in Appendix A.

17.1 Definition For $[a], [b] \in \mathbb{Z}_m$, the *sum* of the residue class $[a]$ and the residue class $[b]$ is the residue class $[a+b]$. The *product* of the residue class $[a]$ and the residue class $[b]$ is the residue class $[ab]$. That is,

$$[a] + [b] = [a+b] \qquad [a][b] = [ab].$$

17.2 Example For $m = 5$ we have $[2] + [3] = [5]$ and $[2][3] = [6]$. Note that since $5 \equiv 0 \pmod 5$ and $6 \equiv 1 \pmod 5$ we can also write $[2] + [3] = [0]$ and $[2][3] = [1]$.

We must check that these binary operations are well defined. That is, since a residue class can have many representatives, we must check that the results of an operation do not depend on the representatives chosen for that operation.

For example, fix $m = 5$ and consider $[7] + [11]$. We know that the residue classes $[7]$ and the residue class $[2]$ are equal, and also that $[11] = [21]$. Therefore for the binary operations to make sense we must have that $[7]+[11] = [2]+[21]$. In this case, $[7] + [11] = [18]$ and $[2] + [21] = [23]$, and $[18] = [23]$ so this one example is fine.

17.3 Theorem The results of the sum and product of residue classes does not depend on the choice of class representative: for any modulus $m > 0$, if $[a] = [b]$ and $[c] = [d]$ then $[a] + [c] = [b] + [d]$ and $[a][c] = [b][d]$.

PROOF. This follows immediately from Theorem 12.6. QED

When performing addition and multiplication in $\mathbb{Z}_m$, we may at any time change class representatives, rewriting $[a]$ by $[a']$, where $a \equiv a' \pmod m$.

17.4 Example Take $m = 151$ and consider the calculation $[150][149]$. Then $150 \equiv -1 \pmod{151}$ and $149 \equiv -2 \pmod{151}$, and so $[150][149] = [-1][-2] = [2]$, an easier calculation.

When working with $\mathbb{Z}_m$ it is often useful to write all residue classes in the least nonnegative residue system, as we do in constructing the following addition and multiplication tables for $\mathbb{Z}_4$.

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Notice that we have reduced results of the sum and product to keep the representative in $[0\,..\,4)$. That is, in constructing those tables we follow the alogrithm that $resclassa + [b] = [(a + b) \bmod m]$ and $[a][b] = [(ab) \bmod m]$.

This leads to an alternative way to define $\mathbb{Z}_m$ and addition and multiplication in $\mathbb{Z}_m$. For clarity we will use different notation.

17.5 Definition For $m > 0$, let J_m be the set $= \{0, 1, 2, \ldots, m-1\}$ endowed with two binary operations: for $a, b \in J_m$, let $a \oplus b = (a + b) \bmod m$ and $a \odot b = (ab) \bmod m$.

Here are the addition and multiplication tables for J_4.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

17.6 Remark The precise expression of the intuition that J_m with $\oplus$ and $\odot$ is just like $\mathbb{Z}_m$ with addition and multiplication is to say that the two are "isomorphic." In this book we will leave the idea as informal.

17.7 Example Let's solve the congruence $272x \equiv 901 \pmod{9}$. Using residue classes modulo 9 we see that this congruence is equivalent to $[272x] = [901]$, which is equivalent to $[272][x] = [901]$. That is equivalent to $[2][x] = [1]$. We know $[x] \in \{[0], [1], \ldots, [8]\}$, so by trial and error we see that $x = 5$ is a solution.

Chapter 18

The Group of Units

This is the multiplication table for $\mathbb{Z}_6$.

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Note that some rows, and some columns, contain all of the members of $\mathbb{Z}_6$ while others do not. We can state that as: for some $[a], [b] \in \mathbb{Z}_6$ the equation $[a] \odot x = [b]$ has no solution x.

18.1 Example The equation $[5] \odot x = [3]$ has the solution $x = [3]$. In fact, for any $[b] \in \mathbb{Z}_6$, the equation $[5] \odot x = [b]$ has a solution. However, the equation $[4] \odot x = [1]$ has no solution.

18.2 Definition Let $m > 0$. A residue class $[a] \in \mathbb{Z}_m$ is a *unit* if there is another residue class $[b] \in \mathbb{Z}_m$ such that $[a] \odot [b] = [1]$. In this case $[a]$ and $[b]$ are said to be *inverses of each other* in $\mathbb{Z}_m$.

18.3 Theorem Let $m > 0$. A residue class $[a] \in \mathbb{Z}_m$ is a unit if and only if $\gcd(a, m) = 1$.

PROOF. Let $[a]$ be a unit. Then there is a $[b]$ such that $[a] \odot [b] = [1]$. Hence $[ab] = [1]$ and so $ab \equiv 1 \pmod{m}$. Thus, by Theorem 14.3, $\gcd(a, m) = 1$.

To prove the converse, let $\gcd(a, m) = 1$. By Theorem 14.1 there is an integer a^* such that $aa^* \equiv 1 \pmod{m}$. Hence $[aa^*] = [1]$. So $[a] \odot [a^*] = [1]$ and we can take $b = a^*$. QED

Note that from Theorem 14.8 if $[a] = [b]$ — that is, if $a \equiv b \pmod{m}$ — then $\gcd(a, m) = 1 \Leftrightarrow \gcd(b, m) = 1$. So, in checking whether or not a residue class is a unit we can use any representative of the class.

18.4 Theorem For $m > 0$, the set of units in Z_m is the set of residue classes $\{[i] \mid 1 \le i \le m \text{ and } \gcd(i, m) = 1\}$.

PROOF. If $[a] \in \mathbb{Z}_m$ then $[a] = [i]$, where $0 \le i \le m - 1$, so for each $m > 0$ we need only consider residue classes with representatives in the interval $[0\,..\,m)$.

If $m = 1$ then $\mathbb{Z}_m$ consists of a single residue class $\mathbb{Z}_1 = \{[0]\} = \{[1]\}$. Since $[1] \odot [1] = [1]$, we have that this single class $[1]$ is a unit.

If $m > 1$ then $\gcd(0, m) = m \neq 1$ and $\gcd(m, m) = m \neq 1$, but $\gcd(i, m) = 1$ for $1 \le i \le m$. So the theorem follows from Theorem 18.3. QED

18.5 Definition The set of all units in $\mathbb{Z}_m$, the *group of units*, is denoted U_m.

(See Appendix A for the definition of a group.)

18.6 Example Here are the first few U_m's.

i	1	2	3	4	5	6
U_i	$\{[1]\}$	$\{[1]\}$	$\{[1], [2]\}$	$\{[1], [3]\}$	$\{[1], [2], [3], [4]\}$	$\{[1], [5]\}$

18.7 Theorem The set of units U_m has these properties.

1. *(Closure)* If $[a]$ and $[b]$ are members of U_m then the product $[a][b]$ is also a member of U_m.
2. *(Associativity)* For all $[a]$, $[b]$, $[c]$ in U_m we have $([a] \odot [b]) \odot [c] = [a] \odot ([b] \odot [c])$.
3. *(Existence of an identity)* $[1] \odot [a] = [a] \odot [1] = [a]$ for all $[a] \in U_m$.
4. *(Existence of inverses)* For each $[a] \in U_m$ there is a $[a]^* \in U_m$ such that $[a] \odot [a]^* = [1]$.
5. *(Commutativity)* For all $[a], [b] \in U_m$, we have that $[a] \odot [b] = [b] \odot [a]$.

18.8 Example Theorem 18.3 shows that

$$\begin{aligned} U_{15} &= \{[1], [2], [4], [7], [8], [11], [13], [14]\} \\ &= \{[1], [2], [4], [7], [-7], [-4], [-2], [-1]\}. \end{aligned}$$

Rather than list the entire multiplication table, we just show the inverse of each element.

r	$[1]$	$[2]$	$[4]$	$[7]$	$[8]$	$[11]$	$[13]$	$[14]$
inverse of r	$[1]$	$[8]$	$[4]$	$[13]$	$[2]$	$[11]$	$[7]$	$[14]$

18.9 Theorem Let $m > 0$ and fix $[a], [b] \in U_m$. Then the equation $[a] \odot x$ *resclassb* has a unique solution $x \in U_m$.

PROOF. To see that it has a solution, consider $[a]^* \odot [b]$. By the closure property, that is an element of U_m. Also, $[a] \odot ([a]^* \odot [b]) = ([a] \odot [a]^*) \odot [b] = [1] \odot [b] = [1 \cdot b] = [b]$, as required (the first equality follows by the associative property).

To see that the solution is unique, suppose that $x, x' \in U_m$ are such that $[a] \odot x = [b]$ and also $[a] \odot x' = [b]$. Then $[a] \odot x = [a] \odot x'$. Multiplying both sides of that equation by the inverse $[a]^*$ gives $[a]^* \odot ([a] \odot x) = ([a]^* \odot [a]) \odot x = [1] \odot x = x$ on the left, and x' on the right. So the two are equal. QED

18.10 Definition If X is a set, the *cardinality* $|X|$ is the number of elements in X.

18.11 Example $|\{1\}| = 1$, $|\{0, 1, 3, 9\}| = 4$, $|\mathbb{Z}_m| = m$ if $m > 0$.

18.12 Definition If $m \geq 1$ then the *Euler phi function* (or the *totient*) is $\phi(m) = |\{i \in \mathbb{Z} \mid 1 \leq i \leq m \text{ and } \gcd(i, m) = 1\}|$.

18.13 Example Here are the first few values of ϕ.

i	1	2	3	4	5	6
$\phi(i)$	1	1	2	2	4	2

Compare this to the table in Example 18.6.

18.14 Corollary If $m > 0$ then $|U_m| = \phi(m)$.

Note that if p is any prime then $\phi(p) = p - 1$.

In general, though, $\phi(m)$ is not easy to calculate. However, computing $\phi(m)$ is easy once we know the prime factorization of m.

18.15 Theorem Fix $a, b > 0$. If $\gcd(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$.

18.16 Theorem If p is prime and $n > 0$ then $\phi\left(p^n\right) = p^n - p^{n-1}$.

18.17 Theorem Let $p_1, p_2, \ldots, p_k$ be distinct primes and let $n_1, n_2, \ldots, n_k$ be positive integers. Then

$$\phi\left(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}\right) = \left(p_1^{n_1} - p_1^{n_1 - 1}\right) \cdots \left(p_k^{n_k} - p_k^{n_k - 1}\right).$$

The proofs of Theorem 18.15 and Theorem 18.17 are routine arguments by induction on n, and are left as exercises.

Proof of Theorem 18.16. We want to count the number of elements in the set $A = \{1, 2, \ldots, p^n\}$ that are relatively prime to p^n. Let B be the set of elements of A that are not relatively prime, that is, that have a factor greater than 1 in common with p^n. The nuber p is prime, so the only factors of p^n are $1, p, \ldots, p^n$, and hence $b = pk$ for some k. It follows that if a number b is an element of B then it has the form $b = kp$ for some $1 \leq k \leq p^{n-1}$. That is, B is a subset of this set: $\{p, 2p, 3p, \ldots, kp, \ldots, p^{n-1}p\}$. But obviously every element of that set is not relatively prime to p^n, so in fact B equals that set.

The number of elements in A is $|A| = p^n$ and the number in B is $|B| = p^{n-1}$, so the number of elements of A that are not in B is $p^n - p^{n-1}$. QED

18.18 Example $\phi(12) = \phi(2^2 \cdot 3) = (2^2 - 2^1)(3^1 - 3^0) = 2 \cdot 2 = 4$

18.19 Example $\phi(9000) = \phi(2^3 \cdot 5^3 \cdot 3^2) = (2^3 - 2^2)(5^3 - 5^2)(3^2 - 3^1) = 4 \cdot 100 \cdot 6 = 2400$

Chapter 19

The Chinese Remainder Theorem

19.1 Definition A *linear congruence* has the form $ax \equiv b \pmod{n}$ where x is a variable.

19.2 Example The linear congruence $2x \equiv 1 \pmod 3$ is solved by $x = 2$ because $2 \cdot 2 = 4 \equiv 1 \pmod 3$. The solution set of that congruence is $\{\dots, 2, 5, 8, 11, \dots\}$.

19.3 Example The congruence $4x \equiv 1 \pmod 2$ has no solution, because $4x$ is even, and so is not congruent to 1, modulo 2.

19.4 Lemma Fix a modulus m and a number a. The congruence $ax \equiv b \pmod m$ has a solution if an only if $\gcd(a, m) \mid b$. If a solution x_0 does exist then, where $d = \gcd(a, b)$, the set of solutions is

$$\{\dots, x_0 + (-m/d), x_0, x_0 + (m/d), x_0 + (2m/d), x_0 + (3m/d), \dots\}$$

the residue class $[x_0]$ modulo m/d.

PROOF. The existence of an x solving $ax \equiv b \pmod m$ is equivalent to the existence of a k such that $ax - b = km$, which in turn is equivalent to the equivalence of a k such that $xa + (-k)m = b$. With that, this result is a restatement of Lemma 5.7. QED

One generalization of Lemma 19.4 is to consider systems of linear congruences. In 1247, Ch'in Chiu-Shao published a solution for a special case of that problem. We first need a preliminary result.

19.5 Lemma If $\gcd(a, b) = 1$ and c is a number such that $a \mid c$ and $b \mid c$ then $ab \mid c$

PROOF. Because $a \mid c$ and $b \mid c$ there are numbers k_a, k_b such that $k_a a = c$ and $k_b b = c$. By Bezout's Lemma, there are s and t such that $as + bt = 1$. Multiply by c to get $cas + cbt = c$. Substitution gives $(k_b b)as + (k_a a)bt = c$. Then ab divides the left side of the equation and so ab must divide the right side, c. QED

19.6 Theorem (Chinese Remainder Theorem) Suppose that $m_1, \ldots, m_n$ are pairwise relatively prime (that is, $\gcd(m_i, m_j) = 1$ whenever $i \neq j$). Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m_1 m_2 \ldots m_n$.

PROOF. Let $M = m_1 m_2 \ldots m_n$ and for $i \in \{1, \ldots, n\}$ let $M_i = M/m_i = m_1 m_2 \ldots m_{i-i} m_{i+1} \ldots m_n$. Observe that $\gcd(M_i, m_i) = 1$ and so Lemma 19.4 says that the linear congruence $M_i x \equiv 1 \pmod{m_i}$ has a set of solutions that is a single congruence class $[x_i]$ modulo m_i.

Now consider the number

$$s_0 = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_n M_n x_n.$$

We claim that s_0 solves the system. For, consider the i-th congruence $x \equiv a_i \pmod{m_i}$. Because m_i divides M_j when $i \neq j$, we have that $s_0 \equiv a_i M_i x_i \pmod{m_i}$. Since x_i was chosen because of the property that $M_i x_i \equiv 1 \pmod{m_i}$, we have that $s_0 \equiv a_i \cdot 1 \equiv a_i \pmod{m_i}$, as claimed.

To finish we must show that the solution is unique modulo M. Suppose that x also solves the system, so that for each $i \in \{1, \ldots, n\}$ we have that $x \equiv a_i \equiv x_0 \pmod{m_i}$. Restated, for each i we have that $n_i \mid (x - x_0)$.

We can now show that $m_1 m_2 \ldots m_n \mid (x - x_0)$. We have that $\gcd(m_1, m_2) = 1$ and $m_1 \mid (x - x_0)$ and $m_2 \mid (x - x_0)$, so the prior lemma applies and we conclude that $m_1 m_2 \mid (x - x_0)$. In this way, we can build up to the entire product $m_1 \ldots m_n$. QED

Chapter 20

Fermat's Little Theorem

20.1 Definition For $[a] \in U_m$, the *powers of the residue class* are given by $[a]^1 = [a]$, $[a]^2 = [a][a]$, etc.

20.2 Lemma If $[a] \in U_m$ then $[a]^n \in U_m$ for $n \geq 1$, and $[a]^n = [a^n]$.

PROOF. We will check this by induction on n. The $n = 1$ base case is trivial: $[a]^1 = [a] = [a^1]$, and by assumption $[a] \in U_m$. For the inductive step, suppose that $[a]^k = [a^k] \in U_m$ for $k \geq 1$ and consider the $k+1$-st power.

$$[a]^{k+1} = [a]^k[a] = [a^k][a] = [a^k a] = [a^{k+1}]$$

By induction the theorem holds for all $n \geq 1$. QED

20.3 Theorem (Euler's Theorem) If $m > 0$, and a is relatively prime to m, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

PROOF. For $m > 0$, we have that $\gcd(a, m) = 1$ if and only if $[a] \in U_m$. The prior result gives that $a^n \equiv 1 \pmod{m} \iff [a^n] = [1] \iff [a]^n = [1]$. Therefore, Euler's Theorem is equivalent to the following: if $m > 0$ and $[a] \in U_m$ then $[a]^{\phi(m)} = [1]$.

We will write $X_1, X_2, \ldots, X_{\phi(m)}$ for the residue classes in U_m.

We first show that if $X \in U_m$ then the set $\mathcal{O} = \{XX_1, XX_2, \ldots, XX_{\phi(m)}\}$ equals the set U_m. Containment one way is easy: any member of $\mathcal{O}$ is a member of U_m by the closure property of Theorem 18.7. For containment the other way, consider $X_i \in U_m$,and note that Theorem 18.9 shows that the equation $X \odot x = X_i$ has a solution $x = X_j$ for some j, so $X_i = XX_j$ is an element of $\mathcal{O}$.

Next, for any $X \in U_m$ consider the product $XX_1XX_2 \cdots XX_{\phi(m)}$. The associative property says that we can parenthesize this term in any way, and the prior paragraph then gives that the product is $(XX_1)(XX_2)\cdots(XX_{\phi(m)}) = X_1X_2\cdots X_{\phi(m)}$.

Finally, let $A = X_1X_2\cdots X_{\phi(m)}$, and for any $X \in U_m$ consider $X^{\phi(m)}A$. The commutative property of Theorem 18.7 gives that

$$X^{\phi(m)}A = X^{\phi(m)}X_1X_2\cdots X_{\phi(m)} = (XX_1)(XX_2)\cdots(XX_{\phi(m)}).$$

The prior paragraph then shows that $X^{\phi(m)}A = A$.

Multiplying both sides of that equation by the inverse A^* of A gives

$$(X^{\phi(m)}A)A^* = X^{\phi(m)}(AA^*) = X^{\phi(m)}[1] = X^{\phi(m)}$$

on the left and $AA^* = [1]$ on the right, as desired. QED

20.4 Example Fix $m = 12$. The positive integers $a < m$ with $\gcd(a, m) = 1$ are 1, 5, 7 and 11, and so $\phi(m) = 4$. We will check Euler's result for all four.

First, $1^4 \equiv 1 \pmod{12}$ is clear. Next, $5^2 \equiv 1 \pmod{12}$ since $12 \mid 25-1$, and so $5^4 \equiv (5^2)^2 \equiv 1^2 \pmod{12}$. From that one, and because $7 \equiv -5 \pmod{12}$ and 4 is even, $7^4 \equiv 5^4 \pmod{12} \equiv 1 \pmod{12}$. And, fourth, $11 \equiv -1 \pmod{12}$ and again since 4 is even we have that $11^4 \equiv (-1)^4 \pmod{12} \equiv 1 \pmod{12}$.

20.5 Theorem (Fermat's Little Theorem) If p is prime, and a is relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$.

PROOF. Where p is prime, $\phi(p) = p - 1$. QED

20.6 Example Fermat's Little Theorem can simplify the computation of $a^n \bmod p$ where p is prime. Recall that if $a^n \equiv r \pmod{p}$ where $0 \leq r < p$, then $a^n \bmod p = r$. We can do two things to simplify the computation: (i) replace a by $a \bmod p$, and (ii) replace n by $n \bmod (p-1)$.

Suppose that we want to calculate $1234^{7865435} \bmod 11$ Note that $1234 \equiv -1 + 2 - 3 + 4 \pmod{11}$, that is, $1234 \equiv 2 \pmod{11}$. Since $\gcd(2, 11) = 1$ we have that $2^{10} \equiv 1 \pmod{11}$. Now $7865435 = (786543) \cdot 10 + 5$ so

$$\begin{aligned} 2^{7865435} &\equiv 2^{(786543)\cdot 10+5} \pmod{11} \\ &\equiv \left(2^{10}\right)^{786543} \cdot 2^5 \pmod{11} \\ &\equiv 1^{786543} \cdot 2^5 \pmod{11} \\ &\equiv 2^5 \pmod{11}, \end{aligned}$$

and $2^5 = 32 \equiv 10 \pmod{11}$. Hence, $1234^{7865435} \equiv 10 \pmod{11}$. It follows that $1234^{7865435} \bmod 11 = 10$.

20.7 Remark Fermat's theorem is called "little " as a contrast with *Fermat's Last Theorem*, which states that $x^n + y^n = z^n$ has no solutions $x, y, z \in \mathbb{N}$ when $n > 2$. For many years this was the most famous unsolved problem in Mathematics, until it was proved by Andrew Wiles in 1995, over 350 years after it was first mentioned by Fermat. Fermat's Little Theorem is much easier to prove, but has more far-reaching consequences for applications to cryptography and secure transmission of data on the Internet.

Chapter 21

Probabilistic Primality Tests

Fermat's Little Theorem says that if p is prime and $1 \leq a \leq p-1$, then $a^{p-1} \equiv 1 \pmod{p}$. It has this converse.

21.1 Theorem If $m \geq 2$ and for all a such that $1 \leq a \leq m-1$ we have $a^{m-1} \equiv 1 \pmod{m}$ then m must be prime.

PROOF. If the hypothesis holds, then for all a with $1 \leq a \leq m-1$, we know that a has an inverse modulo m, namely, a^{m-2}. By Theorem 18.3, this says that for all $1 \leq a \leq m-1$ we have that $\gcd(a, m) = 1$. But this means that m is prime, because if not then we would have $m = ab$ with $1 < a, b < m$, which would mean $\gcd(a, m) = a > 1$. QED

Therefore, one way to check that a number m is prime would be to check that $1^{m-1} \equiv 1 \pmod{m}$, and that $2^{m-1} \equiv 1 \pmod{m}$, ..., and that $m - 1^{m-1} \equiv 1 \pmod{m}$.

This check is a lot of work, but it does have an advantage. Consider $m = 63$. Note that $2^6 = 64 \equiv 1 \pmod{63}$ and raising both sides to the 10-th power gives $2^{60} \equiv 1 \pmod{63}$. Multiplying both sides by 2^2 yields the conclusion that $2^{62} \equiv 4 \pmod{63}$. Since $4 \not\equiv 1 \pmod{63}$ we have that $2^{62} \not\equiv 1 \pmod{63}$. This tells us, without factoring 63, that 63 is not prime.

On the other hand, knowing only that $2^{m-1} \equiv 1 \pmod{m}$ is not enough to show that m is prime. For instance, $2^{m-1} \equiv 1 \pmod{m}$ for the composite number $m = 341$.

Nonetheless, consider only the base $b = 2$. There are 455,052,511 odd primes $p \leq 10^{10}$, all of which satisfy $2^{p-1} \equiv 1 \pmod{p}$. There are only 14,884 composite numbers $2 < m \leq 10^{10}$ that satisfy $2^{m-1} \equiv 1 \pmod{m}$. Thus, for a randome number m with $2 < m \leq 10^{10}$, if m satisfies $2^{m-1} \equiv 1 \pmod{m}$ then the probability that m is prime is

$$\frac{455,052,511}{455,052,511 + 14,884} \approx .999967292.$$

In other words, if we find that $2^{m-1} \equiv 1 \pmod{m}$, then it is highly likely (but not a certainty) that m is prime, at least when $m \leq 10^{10}$. Thus we are led to the following algorithm (expressed in the syntax of Maple).

```
> is_prob_prime:=proc(n)
    if n <=1  or Power(2,n-1) mod n <> 1 then
       return "not prime";
    else
       return "probably prime";
    end if;
 end proc:
```

What happens if we use 3 instead of 2 in the above probabilistic primality test? Or, better yet, what if we evaluate $a^{m-1} \bmod m$ for several different a's?

The number of primes less than 10^6 is $78,498$. The number of numbers $m \leq 10^6$ that are composite and such that $2^{m-1} \equiv 1 \pmod{m}$ is 245. The number of numbers $m \leq 10^6$ that are composite and such that both $2^{m-1} \equiv 1 \pmod{m}$ and $3^{m-1} \equiv 1 \pmod{m}$ is 66. The number of numbers $m \leq 10^6$ that are composite and such that $a^{m-1} \equiv 1 \pmod{m}$ where a is any of the first thirteen primes is 0. (If $m > 10^6$ and $a^{m-1} \equiv 1 \pmod{m}$ for all a in the set of the first thirteen prime then it is highly likely, but not certain, that m is prime.)

That is, if we check for primality by using the scheme of this chapter then we may possibly find out early that the number is not prime, having done very little work. Otherwise, as we work our way through bases $a \in [1\,..\,m)$, calculating whether $a^{m-1} \equiv 1 \pmod{m}$, we gain confidence that m is prime. This is the *Solovay-Strassen pseudoprimality test*.

In practice, there are better probabilistic primality tests than the one described here. For instance, the built-in Maple procedure `isprime` is a very sophisticated probabilistic primality test. So far no one has found an integer n for which `isprime(n)` gives the wrong answer.

Chapter 22

Representations in Other Bases

22.1 Definition Let $b \geq 2$ and $n > 0$. The *base b representation* of n is $n = [a_k, a_{k-1}, \ldots, a_1, a_0]_b$ for some $k \geq 0$, where $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$ and $a_i \in \{0, 1, \ldots, b-1\}$ for $i = 0, 1, \ldots, k$.

22.2 Example (1) $267 = [5, 3, 1]_7$, since $267 = 5 \cdot 7^2 + 3 \cdot 7 + 1$

(2) $147 = [1, 0, 0, 1, 0, 0, 1, 1]_2$, since $147 = 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1$

(3) $4879 = [4, 8, 7, 9]_{10}$, since $4879 = 4 \cdot 10^3 + 8 \cdot 10^2 + 7 \cdot 10 + 9$

(4) $10705679 = [A, 3, 5, B, 0, F]_{16}$, since $10705679 = 10 \cdot 16^5 + 3 \cdot 16^4 + 5 \cdot 16^3 + 11 \cdot 16^2 + 0 \cdot 16 + 15$

Observe that a number's base 10 representation is just its ordinary one.

The representations are said to be in *binary* if $b = 2$, in *ternary* if $b = 3$, in *octal* if $b = 8$, in *decimal* if $b = 10$, and in *hexadecimal* if $b = 16$. If b is understood, especially if $b = 10$, we write $a_k a_{k-1} \cdots a_1 a_0$, without the subscript base. In the case of $b = 16$, which is used frequently in computer science, for the a_i of 10, 11, 12, 13, 14 and 15 we use A, B, C, D, E and F, respectively.

For a fixed base $b > 2$, the numbers a_i's the *digits* of the base b representation. In the binary case, the a_i's are *bits*, a shortening of "binary digits".

22.3 Theorem If $b \geq 2$ then every $n > 0$ has a unique base b representation.

PROOF. To show that a representation exists, iterate the Division Algorithm:

$$\begin{aligned}
n &= bq_0 + r_0 \quad 0 \leq r_0 < b \\
q_0 &= bq_1 + r_1 \quad 0 \leq r_1 < b \\
q_1 &= bq_2 + r_2 \quad 0 \leq r_2 < b \\
&\vdots \\
q_k &= bq_{k+1} + r_{k+1} \quad 0 \leq r_{k+1} < b.
\end{aligned}$$

Note that $n > q_0 > q_1 > \cdots > q_k$. This shows that iteration of the Division Algorithm cannot go on forever, and we must eventually obtain $q_\ell = 0$ for some ℓ, so that $q_{\ell-1} = b \cdot 0 + r_\ell$. We claim that the desired representation is $n = [r_\ell, r_{\ell-1}, \ldots, r_0]$. For, note that $n = bq_0 + r_0$ and $q_0 = bq_1 + r_1$, and hence $n = b(bq_1 + r_1) + r_0 = b^2q_1 + br_1 + r_0$. Continuing in this way we find that $n = b^{\ell+1}q_\ell + b^\ell r_\ell + \cdots + br_1 + r_0$. And, since $q_\ell = 0$ we have

$$(*) \qquad n = b^\ell r_\ell + \cdots + br_1 + r_0,$$

which shows that $n = [r_\ell, \ldots, r_1, r_0]_b$.

To see that this representation is unique, note that from equation $(*)$ we have

$$n = b\left(b^{\ell-1}r_\ell + \cdots + r_1\right) + r_0, \quad 0 \le r_0 < b.$$

Because r_0 is uniquely determined by n, so is the quotient $q = b^{\ell-1}r_\ell + \cdots + r_1$. A similar argument shows that r_1 is uniquely determined. Continuing in this way we see that all the digits $r_\ell, r_{\ell-1}, \ldots, r_0$ are uniquely determined. QED

22.4 Example We find the base 7 representation of 1,749.

$$\begin{aligned} 1749 &= 249 \cdot 7 + 6 \\ 249 &= 35 \cdot 7 + 4 \\ 35 &= 5 \cdot 7 + 0 \\ 5 &= 0 \cdot 7 + 5 \end{aligned}$$

Hence $1749 = [5, 0, 4, 6]_7$.

22.5 Example This finds the binary representation of 137.

$$\begin{aligned} 137 &= 2 \cdot 68 + 1 \\ 68 &= 2 \cdot 34 + 0 \\ 34 &= 2 \cdot 17 + 0 \\ 17 &= 2 \cdot 8 + 1 \\ 8 &= 2 \cdot 4 + 0 \\ 4 &= 2 \cdot 2 + 0 \\ 2 &= 2 \cdot 1 + 0 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

Therefore $137 = [1, 0, 0, 0, 1, 0, 0, 1]_2$.

22.6 Remark We can sometimes "eyeball" the representation in another base of a small number. For instance, we can see how to represent $n = 137$ in binary, without the machinery of the proof. Note that $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, $2^7 = 128$, and $2^8 = 256$. By eye, we spot that the value closest to 137 but not greater than it is 2^7, and we compute that $137 - 2^7 = 9$. The power of 2 closest to it but not above 9 is 2^3, and $9 - 2^3 = 1$. Finally, 1 is a power of 2, since $1 = 2^0$. Therefore $137 = 2^7 + 2^3 + 2^0$ and so $137 = [1, 0, 0, 0, 1, 0, 0, 1]_2$.

Chapter 23

Computation of $a^N \bmod m$

Some Number Theory work involves computing with large numbers. Since computer multiplication of numbers is a slow operation (relative to computer addition), we can ask: where n is any positive integer, what is the smallest number of multiplications required to compute a^n?

For instance, the naive way to calculate 2^8 is to do seven multiplications.

$$\begin{aligned}
2^2 &= 2 \cdot 2 = 4 \\
2^3 &= 2 \cdot 4 = 8 \\
2^4 &= 2 \cdot 8 = 16 \\
2^5 &= 2 \cdot 16 = 32 \\
2^6 &= 2 \cdot 32 = 64 \\
2^7 &= 2 \cdot 64 = 128 \\
2^8 &= 2 \cdot 128 = 256
\end{aligned}$$

In general, computing a^n by this naive method requires $n - 1$ multiplications.

But we can compute 2^8 with only three multiplications

$$\begin{aligned}
2^2 &= 2 \cdot 2 = 4 \\
2^4 &= \left(2^2\right)^2 = 4 \cdot 4 = 16 \\
2^8 &= \left(2^4\right)^2 = 16 \cdot 16 = 256
\end{aligned}$$

If the exponent has the form $n = 2^k$ then this successive squaring method

requires only k-many multiplications.

$$\begin{aligned} a^2 &= a \cdot a \\ a^{2^2} &= (a^2)^2 = a^2 \cdot a^2 \\ a^{2^3} &= (a^{2^2})^2 = a^{2^2} \cdot a^{2^2} \\ &\vdots \\ a^{2^k} &= (a^{2^{k-1}})^2 = a^{2^{k-1}} \cdot a^{2^{k-1}} \end{aligned}$$

This is quite a savings because if $n = 2^k$ then k is generally much smaller than $n - 1$, just as 3 is smaller than 7.

This is the foundation of the *binary method* to compute a^n. It is best explained by example.

23.1 Example To compute 3^{15}, first express the exponent in binary $15 = 2^3 + 2^2 + 2 + 1 = [1, 1, 1, 1]_2$. Thus, $3^{15} = 3^{2^3} \cdot 3^{2^2} \cdot 3^2 \cdot 3$.

Next, we use successive squaring to get the factors in that expansion of 3^{15}.

$$\begin{aligned} 3^2 &= 3 \cdot 3 = 9 \\ 3^{2^2} &= 9 \cdot 9 = 81 \\ 3^{2^3} &= 81 \cdot 81 = 6561 \end{aligned}$$

Putting those factors together

$$\begin{aligned} 3 \cdot 3^2 &= 3 \cdot 9 = 27 \\ (3 \cdot 3^2) \cdot 3^{2^2} &= 27 \cdot 81 = 2187 \\ (3 \cdot 3^2 \cdot 3^{2^2}) 3^{2^3} &= 2187 \cdot 6561 = 14348907 \end{aligned}$$

gives that $3^{15} = 14348907$. This took just six multiplications, while the naive method would have taken fourteen. (Finding the binary representation of 15 took some extra effort, but not much.)

23.2 Theorem Computing x^n using the binary method requires $\lfloor \lg(n) \rfloor$ divisions and at most $2\lfloor \lg(n) \rfloor$ multiplications.

PROOF. If $n = [a_r, \ldots, a_0]_2$ and $a_r = 1$ then $2^r \leq n \leq < 2^{r+1}$. By the familiar properties of any logarithm, $\lg(2^r) \leq \lg(n) < \lg(2^{r+1})$. Since $\lg_2(2^x) = x$ this gives $r \leq \lg(n) < r + 1$, hence $r = \lfloor \lg(n) \rfloor$. Note that r is the number of times we need to divide to get n's binary representation $n = [a_r, \ldots, a_0]_2$.

To compute the powers $x, x^2, x^{2^2}, \ldots, x^{2^r}$ by successive squaring requires $r = \lfloor \lg(n) \rfloor$ multiplications and similarly to compute the product

$$x^{2^r} \cdot x^{a_{r-1} 2^{r-1}} \cdots x^{a_1 2} \cdot x^{a_0}$$

requires r multiplications. So after obtaining the binary representation we need at most $2r = 2\lfloor \lg(n) \rfloor$ multiplications. QED

Note that if we count an application of the Division Algorithm and a multiplication as having the same cost then the above tells us that we need at most $3\lfloor \lg(n) \rfloor$ operations to compute x^n. So, for example, if $n = 10^6$, then $3\lfloor \lg(n) \rfloor = 57$.

To compute $a^n \bmod m$, we use the binary method of exponentiation, with the added refinement that after every multiplication we reduce modulo m. This keeps the products from getting too big for our computer or calculator.

23.3 Example We compute $3^{15} \bmod 10$:

$$\begin{aligned} 3^2 &= 3 \cdot 3 = 9 \equiv 9 \pmod{10} \\ 3^4 &= 9 \cdot 9 = 81 \equiv 1 \pmod{10} \\ 3^8 &\equiv 1 \cdot 1 \equiv 1 \equiv 1 \pmod{10} \end{aligned}$$

and so $3^{15} = 3^8 \cdot 3^4 \cdot 3^2 \cdot 3^1 \equiv 1 \cdot 1 \cdot 9 \cdot 3 = 27 \equiv 7 \pmod{10}$.

Note that $3^{15} \equiv 7 \pmod{10}$. In Example 23.1 we calculated that $3^{15} = 14348907$ which is clearly congruent to 7 mod 10, but the multiplications there were not so easy.

23.4 Example To find $2^{644} \bmod 645$, we first get the binary representation $644 = [1, 0, 1, 0, 0, 0, 0, 1, 0, 0]_2$. That is, $644 = 2^9 + 2^7 + 2^2 = 512 + 128 + 4$. By successive squaring and reducing modulo 645 we get

$$\begin{aligned} 2^2 &= 2 \cdot 2 = 4 \equiv 4 \pmod{645} \\ 2^4 &\equiv 4 \cdot 4 = 16 \equiv 16 \pmod{645} \\ 2^8 &\equiv 16 \cdot 16 = 256 \equiv 256 \pmod{645} \\ 2^{16} &\equiv 256 \cdot 256 = 65,536 \equiv 391 \pmod{645} \\ 2^{32} &\equiv 391 \cdot 391 = 152,881 \equiv 16 \pmod{645} \\ 2^{64} &\equiv 16 \cdot 16 = 256 \equiv 256 \pmod{645} \\ 2^{128} &\equiv 256 \cdot 256 = 65,536 \equiv 391 \pmod{645} \\ 2^{256} &\equiv 391 \cdot 391 = 152,881 \equiv 16 \pmod{645} \\ 2^{512} &\equiv 16 \cdot 16 = 256 \equiv 256 \pmod{645}. \end{aligned}$$

Now $2^{644} = 2^{512} \cdot 2^{128} \cdot 2^4$, and hence $2^{644} \equiv 256 \cdot 391 \cdot 16 \pmod{645}$. So $256 \cdot 391 = 100099 \equiv 121 \pmod{645}$ and $121 \cdot 16 = 1936 \equiv 1 \pmod{645}$. Hence $2^{644} \bmod 645 = 1$.

Chapter 24

Public Key Cryptosystems

Everyone has tried secret codes. A common one is the Caesar cipher: the sender and the recipient agree in advance to express letters as numbers (1 for A, 2 for B, etc.) and also agree to use an encoding that offsets the message; for instance $f(n) = (n + 13) \bmod 26$ offsets the letters by 13. The sender then, in place of transmitting the number n, will transmit $f(n)$ — instead of A, the sender will transmit K, the thirteenth letter. This code is very easy to break, but nonetheless notice that there is a general encryption/decryption scheme of sending offset letters, and within that scheme it relies on the single secret key, the 13.

In 1976, W Diffie and M Hellman proposed a new kind of cryptographic system where there are two keys. A message encrypted with the first key can be decrypted with the second, and a message encrypted with the second key can be decrypted with the first. We will first illustrate some advantages of such a system and then give one way to produce such key pairs.

24.1 Example If two people, Alice and Bob, want to have private communications then each can take a key. Bob alone can read Alice's messages, and Alice alone can read Bob's.

24.2 Example Alice can keep one key a secret, and publish the other key in a public place such as the Internet. Then people who receive an encrypted message that claims to be from Alice can get Alice's public key and try to decrypt the message. If the result is sensible text, then Alice must have been the one who encrypted it, since she kept her other key private. This is *authentication*; her message has been *digitally signed*.

Also, people who want to send a message to Alice in private can encrypt it with her public key. Only she can decrypt it, using her private key.

24.3 Example Key pairs can be used to do things that seem impossible. Suppose that Alice and Bob want to settle a dispute by flipping a coin, but they must do so over the Internet. Each person will flip separately, and they agree that Alice wins if the two coins come out the same while Bob wins if they are

different. However they do not trust each other and so they cannot just email each other the results. How can they agree if neither will believe the other?

Each person generates a key pair. Each then sends the other the message with "heads" or "tails" encrypted using one of their two keys. After that, each person publishes their other key, the one that they did not use to encrypt. The other person can now decrypt the message they've received — they are sure that they are not being cheated because they now have the other person's outcome, albiet encrypted (and the key pairs have the property that finding a new key pair that makes the message decrypt the other way is essentially impossible).

Implicit in these examples are a number of technical requirements on key pairs: from either key we should not be able to find the other, we should not be able to decrypt the message by just trying every possible key, etc. These technical requirements have been met by a number of schemes. The most important is *RSA*, due to R Rivest, A Shamir, and L Adelman in 1977 [11]. This chapter outlines its number-theoretic underpinning.

Assume that our message has been converted to an integer in the set $J_m = \{0, 1, 2, \ldots, m-1\}$ where m is some positive integer to be determined. (For example, we can take the file as a collection of bits and interpret it as a number written in binary.) Generally this is a large integer. We will require two functions:

$$E : J_m \to J_m \ (E \text{ for } \textit{encipher}) \quad \text{and} \quad D : J_m \to J_m \ (D \text{ for } \textit{decipher}).$$

By 'encipher' and 'decipher' we only mean that $D(E(x)) = x$ for all $x \in J_m$.

We first need two statements about congruences.

24.4 Lemma Let $m_1, m_2 \in \mathbb{Z}+$ be relatively prime. Then $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$ if and only if $a \equiv b \pmod{m_1 m_2}$.

PROOF. One direction is easy: if $a \equiv b \pmod{m_1 m_2}$ then there is $k \in \mathbb{Z}$ such that $a - b = k(m_1 m_2)$. Rewriting that as $a - b = (km_1)m_2$ shows that $a - b$ is a multiple of m_2 and so $a \equiv b \pmod{m_2}$. The other equivalence is similar.

If $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$ then there are $k_1, k_2 \in \mathbb{Z}$ such that $a - b = k_1 m_1$ and $a - b = k_2 m_2$. Therefore $k_1 m_1 = k_2 m_2$. This shows that $m_1 \mid k_2 m_2$. As m_1 is relatively prime to m_2, Lemma 5.6 then gives that $m_1 \mid k_2$. Writing $k_2 = km_1$ for some k, and substituting into the earlier equation $a - b = k_2 m_2$ gives that $a - b = km_1 m_2$. Therefore $a - b \mid m_1 m_2$ and so $a \equiv b \pmod{m_1 m_2}$. QED

24.5 Lemma Let p and q be two distinct primes and let $m = pq$. Suppose that e and d are positive integers that are inverses of each other modulo $\phi(m)$. Then $x^{ed} \equiv x \pmod{m}$ for all x.

PROOF. By Theorem 18.17, $\phi(m) = (p-1)(q-1)$. Since $ed \equiv 1 \pmod{\phi(m)}$ we have that $ed - 1 = k\phi(m) = k(p-1)(q-1)$ for some k. Note the $k > 0$ unless $ed = 1$, in which case the theorem is obvious. So we have

$$(*) \qquad ed = k\phi(m) + 1 = k(p-1)(q-1) + 1$$

for some $k > 0$.

We will show that $x^{ed} \equiv x \pmod{b}$ for all x. There are two cases. For the first case, if $\gcd(x, p) = 1$ then by Fermat's Little Theorem we have that $x^{p-1} \equiv 1 \pmod{p}$. Raising both sides of the congruence to the power $(q-1)k$ gives $x^{(p-1)(q-1)k} \equiv 1 \pmod{p}$. Then multiplying by x gives $x^{(p-1)(q-1)k+1} \equiv x \pmod{p}$. That is, by $(*)$

$$(**) \qquad x^{ed} \equiv x \pmod{p}.$$

For the second case, the $\gcd(x, p) = p$ case, the relation $(**)$ is obvious, since then $x \equiv 0 \pmod{p}$.

A similar argument proves that $x^{ed} \equiv x \pmod{q}$ for all x. So by Lemma 24.4 and the fact that $\gcd(p, q) = 1$, we have that $x^{ed} \equiv x \pmod{m}$ for all x. QED

24.6 Theorem Let p and q be two distinct primes, let $m = pq$, and suppose that e and d are positive integers that are inverses of each other modulo $\phi(m)$. Where $J_m = \{0, 1, 2, \ldots, m-1\}$, define $E : J_m \to J_m$ and $D : J_m \to J_m$ by

$$E(x) = x^e \bmod m \quad \text{and} \quad D(x) = x^d \bmod m.$$

Then E and D are inverse functions.

PROOF. It suffices to show that $D(E(x)) = x$ for all $x \in J_m$. Suppose that $x \in J_m$, and that $E(x) = x^e \bmod m = r_1$, and also that $D(r_1) = r_1^d \bmod m = r_2$. We must show that $r_2 = x$. Since $x^e \bmod m = r_1$ we know that $x^e \equiv r_1 \pmod{m}$. Hence $x^{ed} \equiv r_1^d \pmod{m}$. We also know that $r_1^d \equiv r_2 \pmod{m}$ and hence $x^{ed} \equiv r_2 \pmod{m}$. By Lemma 24.5, $x^{ed} \equiv x \pmod{m}$ so we have that $x \equiv r_2 \pmod{m}$. Since both x and r_2 are elements of J_m, both are the principle residue: $x = r_2$. QED

Appendix A

Proof by Induction

Most of the proof methods used in mathematics are instinctive to a person with a talent for the work. This section covers a method, the method of *Mathematical Induction* that is not.

As with all proofs, we will have some assertion to prove. Each assertion will say that something is true for all integers. Thus, we can denote the assertion $P(n)$. Our first example is the proof that for all n, if $n \geq 5$ then $2^n > 5n$.

$$P(n)\text{: } n \geq 5 \Leftrightarrow 2^n > 5n$$

An argument by induction involves two steps. In the base step we show that P is true for some first integer. Typically, that is a straightforward verification. For our example, we show that $P(5)$ is true by just checking that $2^5 = 32$ is indeed greater than $5 \cdot 5 = 25$, which of course it is.

The second step is called the inductive step. We must show that

$$\text{if } P(5), \ldots, P(k) \text{ are all true then } P(k+1) \text{ is also true.}$$

At the end of the proof we will show why this suffices. For the moment note only that we are *not* asserting that $P(5)$, ..., $P(k)$ are in fact all true (as that would be assuming the thing that we are to prove); instead we are proving that if they are true then $P(k+1)$ follows.

To prove this if-then statement, take the inductive hypothesis that $P(5)$, ..., $P(k)$ hold. Then, by the hypothesis that $P(k)$ is true we have $2^k > 5k$, and Multiplying both sides by 2 gives $2^{k+1} > 10k$ We are trying to prove that $2^{k+1} > 5(k+1)$ so if we can show $10k \geq 5k + 5$ then we will be done. Because $k \geq 5$, we have that $5k \geq 5$ and therefore $10k = 5k + 5k \geq 5k + 5 = 5(k+1)$. We have therefore established $P(k+1)$ follows from the inductive hypothesis, as $2^{k+1} > 10k \geq 5(k+1)$. That ends the inductive step.

To see why the two steps togehter prove the assertion, note that we have checked the statement for 5. To see it is true for 6, note that in the inductive step we proved that $P(5) \Leftrightarrow P(6)$. To see that the statement is true for 7, note that we have proved in the inductive step that $P(5)$ and $P(6) \Leftrightarrow P(7)$ (and the

prior sentence shows that $P(6)$ holds). In this way we can see that the statement is true for all numbers $n \geq 5$.

Here is an induction proof that is more streamlined, more like the ones given elsewhere in the book..

1.1 Proposition If $n \geq 5$ then $2^n > 5n$.

PROOF. We prove the proposition by induction on the variable n.

If $n = 5$ then we have $2^5 > 5 \cdot 5$ or $32 > 25$, which is true.

Next, assume the hypothesis that $2^n > 5n$ for $5 \leq n \leq k$. Taking $n = k$ gives that $2^k > 5k$. Multiplying both sides by 2 gives $2^{k+1} > 10k$. Now $10k = 5k + 5k$ and $k \geq 5$, and so $5k \geq 5$. Hence $10k = 5k + 5k \geq 5k + 5 = 5(k + 1)$. It follows that $2^{k+1} > 10k \geq 5(k + 1)$ and therefore $2^{k+1} > 5(k + 1)$.

Hence by mathematical induction we conclude that $2^n > 5n$ for $n \geq 5$. QED

Appendix B

Axioms for $\mathbb{Z}$

The set of *natural numbers* is $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$. The set of *integers* includes the natural numbers and the negative integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \cdots\}$. We sometimes want to restrict our attention to the *positive integers* $\mathbb{Z}^+ = \{1, 2, \cdots\}$.

The *rational numbers* include all of the fractions $\mathbb{Q} = \{n/m \mid n, m \in \mathbb{Z} \text{ and } m \neq 0\}$. The *real numbers* $\mathbb{R}$ enlarge that set with the irrationals (which are too hard to precisely describe here). Note that $\mathbb{Z}^+ \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

In the first chapter we rely on some particularly important properties of $\mathbb{Z}$, the *axioms*.

1. If a, $b \in \mathbb{Z}$, then $a + b$, $a - b$ and $ab \in \mathbb{Z}$. (That is, $\mathbb{Z}$ is *closed* under addition, subtraction and multiplication.)

2. If $a \in \mathbb{Z}$ then there is no $x \in \mathbb{Z}$ such that $a < x < a + 1$.

3. If a, $b \in \mathbb{Z}$ and $ab = 1$, then either $a = b = 1$ or $a = b = -1$.

4. *Laws of Exponents* For $n, m \in \mathbb{N}$ and $a, b \in \mathbb{R}$ with a and b not both 0 we have $(a^n)^m = a^{nm}$ and $(ab)^n = a^n b^n$. and $a^n a^m = a^{n+m}$.

5. *Properties of Inequalities:* For a, b, c in $\mathbb{R}$ the following hold: if $a < b$ and $b < c$, then $a < c$, and if $a < b$ then $a + c < b + c$, and if $a < b$ and $0 < c$ then $ac < bc$, and if $a < b$ and $c < 0$ then $bc < ac$, and finally, given a and b, one and only one of $a = b$, $a < b$, $b < a$ holds.

6. *Well-Ordering Property* Every non-empty subset of $\mathbb{N}$ contains a least element.

7. *Mathematical Induction* Let $P(n)$ be a statement concerning the integer variable n. Let n_0 be any fixed integer. Then $P(n)$ is true for all integers $n \geq n_0$ if both of the following statements hold: (the base step) $P(n)$ is true for $n = n_0$, and (the inductive step) whenever $P(n)$ is true for $n_0 \leq n \leq k$ then $P(n)$ is true for $n = k + 1$.

Appendix C

Some Properties of $\mathbb{R}$

3.1 Definition Where $x \in \mathbb{R}$, the *floor* (or *greatest integer*) $\lfloor x \rfloor$ is the largest integer less than or equal to x. Its *ceiling* $\lceil x \rceil$ is the least integer greater than or equal to x.

For example, $\lfloor 3.1 \rfloor = 3$ and $\lceil 3.1 \rceil = 4$, $\lfloor 3 \rfloor = 3$ and $\lceil 3 \rceil = 3$, and $\lfloor -3.1 \rfloor = -4$ and $\lceil -3.1 \rceil = -3$.

From that definition we immediately have that $\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}$, and that $n = \lfloor x \rfloor \iff n \leq x < n + 1$. From this we have also that $\lfloor x \rfloor \leq x$ and that $\lfloor x \rfloor = x \iff x \in \mathbb{Z}$.

3.2 Lemma (Floor Lemma) Where x is real, $x - 1 < \lfloor x \rfloor \leq x$.

PROOF. Let $n = \lfloor x \rfloor$. Then by the above comments, we have $n \leq x < n + 1$. This gives immediately that $\lfloor x \rfloor \leq x$, as already noted above. It also gives that $x < n + 1$ which implies that $x - 1 < n$, that is, that $x - 1 < \lfloor x \rfloor$. QED

3.3 Definition The *decimal representation* of a positive integer a is given by $a = a_{n-1}a_{n-2} \cdots a_1 a_0$ where

$$a = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0$$

and the *digits* $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ are in the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, with $a_{n-1} \neq 0$. This representation shows that a is, with respect to base 10, an n *digit number* (or is n *digits long*).

Bibliography

[1] Tom Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York-Heidelberg, 1976.

[2] Chris Caldwell, *The Primes Pages*, `http://www.utm.edu/research/primes/`

[3] W. Edwin Clark, *Number Theory Links*, `http://www.math.usf.edu/~eclark/numtheory_links.html`

[4] W Diffie, M Hellman, *New Directions in Cryptography*, *IEEE Transactions on Information Theory* 22 (1976), 644-654.

[5] Earl Fife and Larry Husch, *Number Theory (Mathematics Archives*, `http://archives.math.utk.edu/topics/numberTheory.html`

[6] Ronald Graham, Donald Knuth, and Oren Patashnik, *Concrete Mathematics*, Addison-Wesley, 1994.

[7] Donald Knuth *The Art of Computer Programming*, Vols I and II, Addison-Wesley, 1997.

[8] The Math Forum, *Number Theory Sites* `http://mathforum.org/library/topics/number_theory/`

[9] Oystein Ore, *Number Theory and its History*, Dover Publications, 1988.

[10] Carl Pomerance and Richard Crandall, *Prime Numbers – A Computational Perspective*, Springer -Verlag, 2001.

[11] R Rivest, A Shamir, L Adelman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* available from `http://citeseer.nj.nec.com/rivest78method.html`, 1977

[12] Kenneth A. Rosen, *Elementary Number Theory*, (Fourth Edition), Addison-Wesley, 2000.

[13] Eric Weisstein, *World of Mathematics –Number Theory Section*, `http://mathworld.wolfram.com/topics/NumberTheory.html`

Index