Module MA2C03: Discrete Mathematics
Hilary Term 2016
Section 41 and 42: Number Theory and Cryptography

D. R. Wilkins

Contents

41 Elementary Number Theory

41.1 Subgroups of the Integers

A subset S of the set $\mathbb{Z}$ of integers is a *subgroup* of $\mathbb{Z}$ if $0 \in S$, $-x \in S$ and $x + y \in S$ for all $x \in S$ and $y \in S$.

It is easy to see that a non-empty subset S of $\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ if and only if $x - y \in S$ for all $x \in S$ and $y \in S$.

Let m be an integer, and let $m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$. Then $m\mathbb{Z}$ (the set of integer multiples of m) is a subgroup of $\mathbb{Z}$.

Theorem 41.1 *Let S be a subgroup of $\mathbb{Z}$. Then $S = m\mathbb{Z}$ for some non-negative integer m.*

Proof If $S = \{0\}$ then $S = m\mathbb{Z}$ with $m = 0$. Suppose that $S \neq \{0\}$. Then S contains a non-zero integer, and therefore S contains a positive integer (since $-x \in S$ for all $x \in S$). Let m be the smallest positive integer belonging to S. A positive integer n belonging to S can be written in the form $n = qm + r$, where q is a positive integer and r is an integer satisfying $0 \leq r < m$. Then $qm \in S$ (because $qm = m + m + \cdots + m$). But then $r \in S$, since $r = n - qm$. It follows that $r = 0$, since m is the smallest positive integer in S. Therefore $n = qm$, and thus $n \in m\mathbb{Z}$. It follows that $S = m\mathbb{Z}$, as required. ∎

41.2 Greatest Common Divisors

Definition Let $a_1, a_2, \ldots, a_r$ be integers, not all zero. A *common divisor* of $a_1, a_2, \ldots, a_r$ is an integer that divides each of $a_1, a_2, \ldots, a_r$. The *greatest common divisor* of $a_1, a_2, \ldots, a_r$ is the greatest positive integer that divides each of $a_1, a_2, \ldots, a_r$. The greatest common divisor of $a_1, a_2, \ldots, a_r$ is denoted by $(a_1, a_2, \ldots, a_r)$.

Theorem 41.2 *Let $a_1, a_2, \ldots, a_r$ be integers, not all zero. Then there exist integers $u_1, u_2, \ldots, u_r$ such that*

$$(a_1, a_2, \ldots, a_r) = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r.$$

where $(a_1, a_2, \ldots, a_r)$ is the greatest common divisor of $a_1, a_2, \ldots, a_r$.

Proof Let S be the set of all integers that are of the form

$$n_1 a_1 + n_2 a_2 + \cdots + n_r a_r$$

for some $n_1, n_2, \ldots, n_r \in \mathbb{Z}$. Then S is a subgroup of $\mathbb{Z}$. It follows that $S = m\mathbb{Z}$ for some non-negative integer m (Theorem 41.1). Then m is a common divisor of $a_1, a_2, \ldots, a_r$, (since $a_i \in S$ for $i = 1, 2, \ldots, r$). Moreover any common divisor of $a_1, a_2, \ldots, a_r$ is a divisor of each element of S and is therefore a divisor of m. It follows that m is the greatest common divisor of $a_1, a_2, \ldots, a_r$. But $m \in S$, and therefore there exist integers $u_1, u_2, \ldots, u_r$ such that

$$(a_1, a_2, \ldots, a_r) = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r,$$

as required. ▮

Definition Let $a_1, a_2, \ldots, a_r$ be integers, not all zero. If the greatest common divisor of $a_1, a_2, \ldots, a_r$ is 1 then these integers are said to be *coprime*. If integers a and b are coprime then a is said to be coprime to b. (Thus a is coprime to b if and only if b is coprime to a.)

Corollary 41.3 *Let $a_1, a_2, \ldots, a_r$ be integers that are not all zero. Then $a_1, a_2, \ldots, a_r$ are coprime if and only if there exist integers $u_1, u_2, \ldots, u_r$ such that*

$$1 = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r.$$

Proof If $a_1, a_2, \ldots, a_r$ are coprime then the existence of the required integers $u_1, u_2, \ldots, u_r$ follows from Theorem 41.2. On the other hand, if there exist integers $u_1, u_2, \ldots, u_r$ with the required property then any common divisor of $a_1, a_2, \ldots, a_r$ must be a divisor of 1, and therefore $a_1, a_2, \ldots, a_r$ must be coprime. ▮

41.3 The Euclidean Algorithm

Let a and b be positive integers with $a > b$. Let $r_0 = a$ and $r_1 = b$. If b does not divide a then let r_2 be the remainder on dividing a by b. Then $a = q_1 b + r_2$, where q_1 and r_2 are positive integers and $0 < r_2 < b$. If r_2 does not divide b then let r_3 be the remainder on dividing b by r_2. Then $b = q_2 r_2 + r_3$, where q_2 and r_3 are positive integers and $0 < r_3 < r_2$. If r_3 does not divide r_2 then let r_4 be the remainder on dividing r_2 by r_3. Then $r_2 = q_3 r_3 + r_4$, where q_3 and r_4 are positive integers and $0 < r_4 < r_3$. Continuing in this fashion, we construct positive integers $r_0, r_1, \ldots, r_n$ such that $r_0 = a$, $r_1 = b$ and r_i is the remainder on dividing r_{i-2} by r_{i-1} for $i = 2, 3, \ldots, n$. Then $r_{i-2} = q_{i-1} r_{i-1} + r_i$, where q_{i-1} and r_i are positive integers and $0 < r_i < r_{i-1}$. The algorithm for constructing the positive integers $r_0, r_1, \ldots, r_n$ terminates when r_n divides r_{n-1}. Then $r_{n-1} = q_n r_n$ for some positive integer q_n. (The algorithm must clearly terminate in a finite number of steps, since $r_0 > r_1 > r_2 > \cdots > r_n$.)

We claim that r_n is the greatest common divisor of a and b.

Any divisor of r_n is a divisor of r_{n-1}, because $r_{n-1} = q_n r_n$. Moreover if $2 \leq i \leq n$ then any common divisor of r_i and r_{i-1} is a divisor of r_{i-2}, because $r_{i-2} = q_{i-1} r_{i-1} + r_i$. If follows that every divisor of r_n is a divisor of all the integers $r_0, r_1, \ldots, r_n$. In particular, any divisor of r_n is a common divisor of a and b. In particular, r_n is itself a common divisor of a and b.

If $2 \leq i \leq n$ then any common divisor of r_{i-2} and r_{i-1} is a divisor of r_i, because $r_i = r_{i-2} - q_{i-1} r_{i-1}$. It follows that every common divisor of a and b is a divisor of all the integers $r_0, r_1, \ldots, r_n$. In particular any common divisor of a and b is a divisor of r_n. It follows that r_n is the greatest common divisor of a and b.

There exist integers u_i and v_i such that $r_i = u_i a + v_i b$ for $i = 1, 2, \ldots, n$. Indeed $u_i = u_{i-2} - q_{i-1} u_{i-1}$ and $v_i = v_{i-2} - q_{i-1} v_{i-1}$ for each integer i between 2 and n, where $u_0 = 1$, $v_0 = 0$, $u_1 = 0$ and $v_1 = 1$. In particular $r_n = u_n a + v_n b$.

The algorithm described above for calculating the greatest common divisor (a, b) of two positive integers a and b is referred to as the *Euclidean algorithm*. It also enables one to calculate integers u and v such that $(a, b) = ua + vb$.

Example We calculate the greatest common divisor of 425 and 119. Now

$$\begin{aligned} 425 &= 3 \times 119 + 68 \\ 119 &= 68 + 51 \\ 68 &= 51 + 17 \\ 51 &= 3 \times 17. \end{aligned}$$

It follows that 17 is the greatest common divisor of 425 and 119. Moreover

$$\begin{aligned} 17 &= 68 - 51 = 68 - (119 - 68) \\ &= 2 \times 68 - 119 = 2 \times (425 - 3 \times 119) - 119 \\ &= 2 \times 425 - 7 \times 119. \end{aligned}$$

Example We calculate the greatest common divisor of 90, 126, 210, and express it in the form $90u + 126v + 210w$ for appropriate integers u, v and w.

First we calculate the greatest common divisor of 90 and 126 using the Euclidean algorithm. Now

$$\begin{aligned} 126 &= 90 + 36 \\ 90 &= 2 \times 36 + 18 \\ 36 &= 2 \times 18. \end{aligned}$$

It follows that 18 is the greatest common divisor of 90 and 126. Moreover

$$\begin{aligned} 18 &= 90 - 2 \times 36 = 90 - 2 \times (126 - 90) \\ &= 3 \times 90 - 2 \times 126. \end{aligned}$$

Now any common divisor d of 90, 126 and 210 is a common divisor of 90 and 126, and therefore divides the greatest common divisor of 90 and 126. Thus d divides 18. But d also divides 210. It follows that any common divisor of 90, 126 and 210 is a common divisor of 18 and 210, and therefore divides the greatest common divisor of 18 and 210. We calculate this greatest common divisor using the Euclidean algorithm. Now

$$\begin{aligned} 210 &= 11 \times 18 + 12 \\ 18 &= 12 + 6 \\ 12 &= 2 \times 6. \end{aligned}$$

It follows that 6 is the greatest common divisor of 18 and 210. Moreover

$$\begin{aligned} 6 &= 18 - 12 = 18 - (210 - 11 \times 18) \\ &= 12 \times 18 - 210. \end{aligned}$$

But $18 = 3 \times 90 - 2 \times 126$. It follows that

$$6 = 36 \times 90 - 24 \times 126 - 210.$$

The number 6 divides 90, 126 and 210. Moreover any common divisor of 90, 126 and 210 must also divide 6. Therefore 6 is the greatest common divisor of 90, 126 and 210. Also $6 = 90u + 126v + 210w$ where $u = 36$, $v = -24$ and $w = -1$.

Remark Let $a_1, a_2, \ldots, a_r$ be non-zero integers, where $r > 2$. Suppose we wish to compute the greatest common divisor d of $a_1, a_2, \ldots, a_r$, and express it in the form

$$d = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r.$$

where $u_1, u_2, \ldots, u_r$ are integers.

Let d' be the greatest common divisor of $a_1, a_2, \ldots, a_{r-1}$. Then any common divisor of $a_1, a_2, \ldots, a_r$ divides both d' and a_r, and therefore divides the greatest common divisor (d', a_r) of d' and a_r. In particular d divides (d', a_r). But (d', a_r) divides a_i for $i = 1, 2, \ldots, r$. It follows that $d = (d', a_r)$. Thus

$$(a_1, a_2, \ldots, a_r) = ((a_1, a_2, \ldots, a_{r-1}), a_r).$$

for any non-zero integers $a_1, a_2, \ldots, a_r$. Moreover there exist integers p and q such that $d = pd' + qa_r$. These integers p and q may be computed using the Euclidean algorithm, given d' and a_r.

Let $v_1, v_2, \ldots, v_{r-1}$ be integers for which

$$d' = v_1 a_1 + v_2 a_2 + \cdots + v_{r-1} a_{r-1}.$$

Then

$$d = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r,$$

where $u_i = pv_i$ for $i = 1, 2, \ldots, r-1$ and $u_r = q$. Therefore successive applications of the Euclidean algorithm will enable us to compute the greatest common divisor $(a_1, a_2, \ldots, a_r)$ of $a_1, a_2, \ldots, a_r$ and express it in the form

$$(a_1, a_2, \ldots, a_r) = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r$$

for appropriate integers $u_1, u_2, \ldots, u_r$.

Indeed we may proceed by computing successively the greatest common divisors

$$(a_1, a_2), \ (a_1, a_2, a_3), \ (a_1, a_2, a_3, a_4), \ldots,$$

representing each quantity $(a_1, a_2, \ldots, a_k)$ by an expression of the form

$$(a_1, a_2, \ldots, a_k) = \sum_{i=1}^{k} v_{ki} a_i,$$

where the quantities v_{ki} are integers.

41.4 Prime Numbers

Definition A *prime number* is an integer p greater than one with the property that 1 and p are the only positive integers that divide p.

Let p be a prime number, and let x be an integer. Then the greatest common divisor (p, x) of p and x is a divisor of p, and therefore either $(p, x) = p$ or else $(p, x) = 1$. It follows that either x is divisible by p or else x is coprime to p.

Theorem 41.4 *Let p be a prime number, and let x and y be integers. If p divides xy then either p divides x or else p divides y.*

Proof Suppose that p divides xy but p does not divide x. Then p and x are coprime, and hence there exist integers u and v such that $1 = up + vx$ (Corollary 41.3). Then $y = upy + vxy$. It then follows that p divides y, as required. ∎

Corollary 41.5 *Let p be a prime number. If p divides a product of integers then p divides at least one of the factors of the product.*

Proof Let $a_1, a_2, \ldots, a_k$ be integers, where $k > 1$. Suppose that p divides $a_1 a_2 \cdots a_k$. Then either p divides a_k or else p divides $a_1 a_2 \cdots a_{k-1}$. The required result therefore follows by induction on the number k of factors in the product. ∎

41.5 The Fundamental Theorem of Arithmetic

Lemma 41.6 *Every integer greater than one is a prime number or factors as a product of prime numbers.*

Proof Let n be an integer greater than one. Suppose that every integer m satisfying $1 < m < n$ is a prime number or factors as a product of prime numbers. If n is not a prime number then $n = ab$ for some integers a and b satisfying $1 < a < n$ and $1 < b < n$. Then a and b are prime numbers or products of prime numbers. Thus if n is not itself a prime number then n must be a product of prime numbers. The required result therefore follows by induction on n. ∎

An integer greater than one that is not a prime number is said to be a *composite number*.

Let n be an composite number. We say that n factors uniquely as a product of prime numbers if, given prime numbers $p_1, p_2, \ldots, p_r$ and $q_1, q_2, \ldots, q_s$ such that

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \ldots q_s,$$

the number of times a prime number occurs in the list $p_1, p_2, \ldots, p_r$ is equal to the number of times it occurs in the list $q_1, q_2, \ldots, q_s$. (Note that this implies that $r = s$.)

Theorem 41.7 (The Fundamental Theorem of Arithmetic) *Every composite number greater than one factors uniquely as a product of prime numbers.*

Proof Let n be a composite number greater than one. Suppose that every composite number greater than one and less than n factors uniquely as a product of prime numbers. We show that n then factors uniquely as a product of prime numbers. Suppose therefore that

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \ldots, q_s,$$

where $p_1, p_2, \ldots, p_r$ and $q_1, q_2, \ldots, q_s$ are prime numbers, $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$. We must prove that $r = s$ and $p_i = q_i$ for all integers i between 1 and r.

Let p be the smallest prime number that divides n. If a prime number divides a product of integers then it must divide at least one of the factors (Corollary 41.5). It follows that p must divide p_i and thus $p = p_i$ for some integer i between 1 and r. But then $p = p_1$, since p_1 is the smallest of the prime numbers $p_1, p_2, \ldots, p_r$. Similarly $p = q_1$. Therefore $p = p_1 = q_1$. Let $m = n/p$. Then

$$m = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

But then $r = s$ and $p_i = q_i$ for all integers i between 2 and r, because every composite number greater than one and less than n factors uniquely as a product of prime numbers. It follows that n factors uniquely as a product of prime numbers. The required result now follows by induction on n. (We have shown that if all composite numbers m satisfying $1 < m < n$ factor uniquely as a product of prime numbers, then so do all composite numbers m satisfying $1 < m < n + 1$.) ∎

41.6 The Infinitude of Primes

Theorem 41.8 (Euclid) *The number of prime numbers is infinite.*

Proof Let $p_1, p_2, \ldots, p_r$ be prime numbers, let $m = p_1 p_2 \cdots p_r + 1$. Now p_i does not divide m for $i = 1, 2, \ldots, r$, since if p_i were to divide m then it would divide $m - p_1 p_2 \cdots p_r$ and thus would divide 1. Let p be a prime factor of m. Then p must be distinct from $p_1, p_2, \ldots, p_r$. Thus no finite set $\{p_1, p_2, \ldots, p_r\}$ of prime numbers can include all prime numbers. ∎

41.7 Congruences

Let m be a positive integer. Integers x and y are said to be *congruent* modulo m if $x - y$ is divisible by m. If x and y are congruent modulo m then we denote this by writing $x \equiv y \pmod{m}$.

The *congruence class* of an integer x modulo m is the set of all integers that are congruent to x modulo m.

Let x, y and z be integers. Then $x \equiv x \pmod{m}$. Also $x \equiv y \pmod{m}$ if and only if $y \equiv x \pmod{m}$. If $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$ then $x \equiv z \pmod{m}$. Thus congruence modulo m is an equivalence relation on the set of integers.

Lemma 41.9 *Let m be a positive integer, and let x, x', y and y' be integers. Suppose that $x \equiv x' \pmod{m}$ and $y \equiv y' \pmod{m}$. Then $x + y \equiv x' + y' \pmod{m}$ and $xy \equiv x'y' \pmod{m}$.*

Proof The result follows immediately from the identities

$$\begin{aligned} (x + y) - (x' + y') &= (x - x') + (y - y'), \\ xy - x'y' &= (x - x')y + x'(y - y'). \quad \blacksquare \end{aligned}$$

Lemma 41.10 *Let x, y and m be integers with $m \neq 0$. Suppose that m divides xy and that m and x are coprime. Then m divides y.*

Proof There exist integers a and b such that $1 = am + bx$, since m and x are coprime (Corollary 41.3). Then $y = amy + bxy$, and m divides xy, and therefore m divides y, as required. $\blacksquare$

Lemma 41.11 *Let m be a positive integer, and let a, x and y be integers with $ax \equiv ay \pmod{m}$. Suppose that m and a are coprime. Then $x \equiv y \pmod{m}$.*

Proof If $ax \equiv ay \pmod{m}$ then $a(x - y)$ is divisible by m. But m and a are coprime. It therefore follows from Lemma 41.10 that $x - y$ is divisible by m, and thus $x \equiv y \pmod{m}$, as required. $\blacksquare$

Lemma 41.12 *Let x and m be non-zero integers. Suppose that x is coprime to m. Then there exists an integer y such that $xy \equiv 1 \pmod{m}$. Moreover y is coprime to m.*

Proof There exist integers y and k such that $xy + mk = 1$, since x and m are coprime (Corollary 41.3). Then $xy \equiv 1 \pmod{m}$. Moreover any common divisor of y and m must divide xy and therefore must divide 1. Thus y is coprime to m, as required. $\blacksquare$

Lemma 41.13 *Let m be a positive integer, and let a and b be integers, where a is coprime to m. Then there exist integers x that satisfy the congruence $ax \equiv b \pmod{m}$. Moreover if x and x' are integers such that $ax \equiv b \pmod{m}$ and $ax' \equiv b \pmod{m}$ then $x \equiv x' \pmod{m}$.*

Proof There exists an integer c such that $ac \equiv 1 \pmod{m}$, since a is coprime to m (Lemma 41.12). Then $ax \equiv b \pmod{m}$ if and only if $x \equiv cb \pmod{m}$. The result follows. $\blacksquare$

Lemma 41.14 *Let $a_1, a_2, \ldots, a_r$ be integers, and let x be an integer that is coprime to a_i for $i = 1, 2, \ldots, r$. Then x is coprime to the product $a_1 a_2 \cdots a_r$ of the integers $a_1, a_2, \ldots, a_r$.*

Proof Let p be a prime number which divides the product $a_1 a_2 \cdots a_r$. Then p divides one of the factors $a_1, a_2, \ldots, a_r$ (Corollary 41.5). It follows that p cannot divide x, since x and a_i are coprime for $i = 1, 2, \ldots, r$. Thus no prime number is a common divisor of x and the product $a_1 a_2 \cdots a_r$. It follows that the greatest common divisor of x and $a_1 a_2 \cdots a_r$ is 1, since this greatest common divisor cannot have any prime factors. Thus x and $a_1 a_2 \cdots a_r$ are coprime, as required. ∎

Let m be a positive integer. For each integer x, let $[x]$ denote the congruence class of x modulo m. If x, x', y and y' are integers and if $x \equiv x' \pmod{m}$ and $y \equiv y' \pmod{m}$ then $xy \equiv x'y' \pmod{m}$. It follows that there is a well-defined operation of multiplication defined on congruence classes of integers modulo m, where $[x][y] = [xy]$ for all integers x and y. This operation is commutative and associative, and $[x][1] = [x]$ for all integers x. If x is an integer coprime to m, then it follows from Lemma 41.12 that there exists an integer y coprime to m such that $xy \equiv 1 \pmod{m}$. Then $[x][y] = [1]$. Therefore the set $\mathbb{Z}_m^*$ of congruence classes modulo m of integers coprime to m is an Abelian group (with multiplication of congruence classes defined as above).

41.8 Computing Powers in Modular Arithmetic

Let m be a positive integer, and let a be an integer. Suppose that one wishes to calculate the value of a^n modulo m, where n is some large positive integer. It is not computationally efficient to calculate the value of a^n for a large value of n and then reduce the value of this integer modulo m.

Instead one may proceed by calculating a sequence

$$a_0, a_1, a_2, a_3, \ldots$$

of integers, where $a_0 \equiv a \pmod{m}$ $0 \leq a_i < m$ and $a_{i+1} \equiv a_i^2 \pmod{m}$ for $i = 0, 1, 2, 3, \ldots$. Now $a^{2^{i+1}} = (a^{2^i})^2$ for all non-negative integers i. It then follows from Lemma 41.9 and the Principle of Mathematical Induction that $a^{2^i} \equiv a_i \pmod{m}$ for all non-negative integers i. Thus the members of the sequence $a_0, a_1, a_2, a_3, \ldots$ are congruent modulo m to those values of a^n for which n is a non-negative power of 2.

Now any positive integer may be expressed as a sum of powers of two. Indeed let n be a positive integer, and let the digits in the standard binary representation of n, read from right to left, be $e_0, e_1, \ldots, e_r$, where e_0 is the least significant digit, e_r is the most significant digit, and e_i is equal either to 0 or to 1 for $i = 0, 1, \ldots, r$. Then $n = \sum_{i=0}^{k} e_i 2^i$, and thus n is the sum of those powers 2^i of two for which $e_i = 1$.

Let $n = 2^{k_1} + 2^{k_2} + \cdots 2^{k_m}$, where $k_1, k_2, \ldots, k_m$ are distinct non-negative integers. Then $a^n = a^{2^{k_1}} a^{2^{k_2}} \cdots a^{2^{k_m}}$. It then follows from Lemma 41.9 that $a^n \equiv a_{k_1} a_{k_2} \cdots a_{k_m} \pmod{m}$, where $0 \leq a_i < m$ and $a_i \equiv a^{2^i} \pmod{m}$ for all non-negative integers i.

Example We calculate $58^n \pmod{221}$ where

$$\begin{aligned} n &= 2^{176} \\ &= 95780971304118053647396689196894323976171195136475136. \end{aligned}$$

Let $a_0 = 58$ and let $0 \leq a_{i+1} < 221$ and $a_{i+1} \equiv a_i^2 \pmod{221}$ for all non-negative integers i. Then

$$a_0 = 58, \quad a_1 = 49, \quad a_2 = 191, \quad a_3 = 16, \quad a_4 = 35, \quad a_5 = 120, a_6 = 35.$$

Note that $a_4 = a_6$. The definition of the numbers a_i then ensures that $a_{4+j} = a_{6+j}$ for all non-negative integers. It follows from this that $a_i = 35$ when i is even and $i \geq 4$, and $a_i = 120$ when i is odd and $i \geq 5$. In particular $58^n \equiv 35 \pmod{221}$ when $n = 2^{176}$, since $58^n \equiv a_{176} \pmod{221}$ and $a_{176} = 35$.

Let m be a positive integer, let a be an integer satisfying $0 \leq a < m$, and let the infinite sequence $a_0, a_1, a_2, a_3, \ldots$ of integers be defined such that $a_0 = a$, $0 \leq a_{i+1} < m$ and $a_{i+1} \equiv a_i^2 \pmod{m}$ for all non-negative integers i. Now the integers a_i can only take on m possible values. It follows that there must exist a non-negative integer r and a strictly positive integer p such that $a_r = a_{r+p}$. But it then follows from the definition of the integers a_i that $a_{r+j} = a_{r+p+j}$ for all non-negative integers j. A straightforward proof by induction on k shows that $a_{r+kp+j} = a_{r+j}$ for all non-negative integers j and k. Thus the values of the sequence $a_r, a_{r+1}, a_{r+2}, \ldots$ are periodic, with period equal to or dividing p, and therefore the values of a_i for $i \geq r$ are completely determined by the values of a_i for $r \leq i < r + p$.

Example We consider the value of $1234^n \pmod{13039}$ for some large integer values of n. We define a sequence $a_0, a_1, a_2, a_3, \ldots$ of integers satisfying $0 \leq a_i < 13039$, where $a_0 = 1234$ and $a_{i+1} \equiv a_i^2 \pmod{13039}$. Calculations show that $a_4 = a_{32} = 10167$. However $a_i \neq 10167$ when $4 < i < 32$. Therefore the sequence of values a_i for $i \geq 4$ is periodic, with period 28, so that $a_{i+28k} = a_i$ for all non-negative integers i and k with $i \geq 4$. The values of a_i for all non-negative integers i are thus determined by the values of a_i for which $0 \leq i < 32$.

We now calculate the value of $1234^n \pmod{13039}$ when

$$n = 18898689444252923985920.$$

Now $n = 2^{47} + 2^{63} + 2^{74}$. It follows that $1234^n \equiv a_{47}a_{63}a_{74} \pmod{13039}$. Moreover $a_{47} = a_{19} = 11935$, $a_{63} = a_7 = 3758$ and $a_{74} = a_{18} = 2211$. Now $11935 \times 3758 \times 2211 \equiv 12377 \pmod{13039}$. We conclude therefore that $1234^n \equiv 12377 \pmod{13039}$. We note also $1234^n > 2^{10n}$. It is not feasable to write out or print the binary or decimal representation of such a large number!

41.9 The Chinese Remainder Theorem

Let I be a set of integers. The integers belonging to I are said to be *pairwise coprime* if any two distinct integers belonging to I are coprime.

Proposition 41.15 *Let $m_1, m_2, \ldots, m_r$ be non-zero integers that are pairwise coprime. Let x be an integer that is divisible by m_i for $i = 1, 2, \ldots, r$. Then x is divisible by the product $m_1m_2 \cdots m_r$ of the integers $m_1, m_2, \ldots, m_r$.*

Proof For each integer k between 1 and r let P_k be the product of the integers m_i with $1 \leq i \leq k$. Then $P_1 = m_1$ and $P_k = P_{k-1}m_k$ for $k = 2, 3, \ldots, r$. Let x be a positive integer that is divisible by m_i for $i = 1, 2, \ldots, r$. We must show that P_r divides x. Suppose that P_{k-1} divides x for some integer k between 2 and r. Let $y = x/P_{k-1}$. Then m_k and P_{k-1} are coprime (Lemma 41.14) and m_k divides $P_{k-1}y$. It follows from Lemma 41.10 that m_k divides y. But then P_k divides x, since $P_k = P_{k-1}m_k$ and $x = P_{k-1}y$. On successively applying this result with $k = 2, 3, \ldots, r$ we conclude that P_r divides x, as required. ∎

Theorem 41.16 (Chinese Remainder Theorem) *Let $m_1, m_2, \ldots, m_r$ be pairwise coprime positive integers. Then, given any integers $x_1, x_2, \ldots, x_r$, there exists an integer z such that $z \equiv x_i \pmod{m_i}$ for $i = 1, 2, \ldots, r$. Moreover if z' is any integer satisfying $z' \equiv x_i \pmod{m_i}$ for $i = 1, 2, \ldots, r$ then $z' \equiv z \pmod{m}$, where $m = m_1m_2 \cdots m_r$.*

Proof Let $m = m_1m_2 \cdots m_r$, and let $s_i = m/m_i$ for $i = 1, 2, \ldots, r$. Note that s_i is the product of the integers m_j with $j \neq i$, and is thus a product of integers coprime to m_i. It follows from Lemma 41.14 that m_i and s_i are coprime for $i = 1, 2, \ldots, r$. Therefore there exist integers a_i and b_i such that $a_i m_i + b_i s_i = 1$ for $i = 1, 2, \ldots, r$ (Corollary 41.3). Let $u_i = b_i s_i$ for $i = 1, 2, \ldots, r$. Then $u_i \equiv 1 \pmod{m_i}$, and $u_i \equiv 0 \pmod{m_j}$ when $j \neq i$. Thus if

$$z = x_1 u_1 + x_2 u_2 + \cdots x_r u_r$$

then $z \equiv x_i \pmod{m_i}$ for $i = 1, 2, \ldots, r$.

Now let z' be an integer with $z' \equiv x_i \pmod{m_i}$ for $i = 1, 2, \ldots, r$. Then $z' - z$ is divisible by m_i for $i = 1, 2, \ldots, r$. It follows from Proposition 41.15 that $z' - z$ is divisible by the product m of the integers $m_1, m_2, \ldots, m_r$. Then $z' \equiv z \pmod{m}$, as required. ∎

Example Suppose we seek an integer x such that $x \equiv 3 \pmod 5$, $x \equiv 7 \pmod{11}$ and $x \equiv 4 \pmod{17}$. (Note that 5, 11 and 17 are prime numbers, and are therefore pairwise coprime.) There should exist such an integer x that is of the form

$$x = 3u_1 + 7u_2 + 4u_3,$$

where

$$\begin{aligned} u_1 \equiv 1 \pmod 5 \quad & u_1 \equiv 0 \pmod{11}, u_1 \equiv 0 \pmod{17}, \\ u_2 \equiv 0 \pmod 5 \quad & u_2 \equiv 1 \pmod{11}, u_2 \equiv 0 \pmod{17}, \\ u_3 \equiv 0 \pmod 5 \quad & u_3 \equiv 0 \pmod{11}, u_3 \equiv 1 \pmod{17}. \end{aligned}$$

Now u_1 should be divisible by both 11 and 17. Moreover 11 and 17 are coprime. It follows that u_1 should be divisible by the product of 11 and 17, which is 187. Now $187 \equiv 2 \pmod 5$, and we are seeking an integer u_1 for which $u_1 \equiv 1 \pmod 5$. However $3 \times 2 = 6$ and $6 \equiv 1 \pmod 5$, and $3 \times 187 = 561$. It follows from standard properties of congruences that if we take $u_1 = 561$, then u_1 satisfies all the required congruences. And one can readily check that this is the case.

Similarly u_2 should be a multiple of 85, given that $85 = 5 * 17$. But $85 \equiv 8 \pmod{11}$, $7 \times 8 = 56$, $56 \equiv 1 \pmod{11}$, and $7 \times 85 = 595$, so if we take $u_2 = 595$ then u_2 should satisfy all the required congruences, and this is the case.

The same method shows that u_3 should be a multiple of 55. But $55 \equiv 4 \pmod{17}$, $13 \times 4 = 52$, $52 \equiv 1 \pmod{17}$ and $13 \times 55 = 715$, and thus if $u_3 = 715$ then u_3 should satisfy the required congruences, which it does.

An integer x satisfying the congruences $x \equiv 3 \pmod 5$, $x \equiv 7 \pmod{11}$ and $x \equiv 4 \pmod{17}$, is then given by

$$x = 3 \times 561 + 7 \times 595 + 4 \times 715 = 8708.$$

Now the integers y satisfying the required congruences are those that satisfy the congruence $y \equiv x \pmod{935}$, since $935 = 5 \times 11 \times 17$. The smallest positive value of y with the required properties is 293.

41.10 Fermat's Little Theorem

Theorem 41.17 (Fermat's Little Theorem) *Let p be a prime number. Then $x^p \equiv x \pmod{p}$ for all integers x. Moreover if x is coprime to p then $x^{p-1} \equiv 1 \pmod{p}$.*

We shall give two proofs of this theorem below.

Lemma 41.18 *Let p be a prime number. Then the binomial coefficient $\binom{p}{k}$ is divisible by p for all integers k satisfying $0 < k < p$.*

Proof The binomial coefficient is given by the formula $\binom{p}{k} = \dfrac{p!}{(p-k)!k!}$. Thus if $0 < k < p$ then $\binom{p}{k} = \dfrac{pm}{k!}$, where $m = \dfrac{(p-1)!}{(p-k)!}$. Thus if $0 < k < p$ then $k!$ divides pm. Also $k!$ is coprime to p. It follows that $k!$ divides m (Lemma 41.10), and therefore the binomial coefficient $\binom{p}{k}$ is a multiple of p. ∎

First Proof of Theorem 41.17 Let p be prime number. Then

$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k.$$

It then follows from Lemma 41.18 that $(x+1)^p \equiv x^p + 1 \pmod{p}$. Thus if $f(x) = x^p - x$ then $f(x+1) \equiv f(x) \pmod{p}$ for all integers x, since $f(x+1) - f(x) = (x+1)^p - x^p - 1$. But $f(0) \equiv 0 \pmod{p}$. It follows by induction on $|x|$ that $f(x) \equiv 0 \pmod{p}$ for all integers x. Thus $x^p \equiv x \pmod{p}$ for all integers x. Moreover if x is coprime to p then it follows from Lemma 41.11 that $x^{p-1} \equiv 1 \pmod{p}$, as required. ∎

Second Proof of Theorem 41.17 Let x be an integer. If x is divisible by p then $x \equiv 0 \pmod{p}$ and $x^p \equiv 0 \pmod{p}$.

Suppose that x is coprime to p. If j is an integer satisfying $1 \leq j \leq p-1$ then j is coprime to p and hence xj is coprime to p. It follows that there exists a unique integer u_j such that $1 \leq u_j \leq p-1$ and $xj \equiv u_j \pmod{p}$. If j and k

are integers between 1 and $p-1$ and if $j \neq k$ then $u_j \neq u_k$. It follows that each integer between 1 and $p-1$ occurs exactly once in the list $u_1, u_2, \ldots, u_{p-1}$, and therefore $u_1 u_2 \cdots u_{p-1} = (p-1)!$. Thus if we multiply together the left hand sides and right hand sides of the congruences $xj \equiv u_j \pmod{p}$ for $j = 1, 2, \ldots, p-1$ we obtain the congruence $x^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. But then $x^{p-1} \equiv 1 \pmod{p}$ by Lemma 41.11, since $(p-1)!$ is coprime to p. But then $x^p \equiv x \pmod{p}$, as required. ∎

42 The RSA Cryptographic System

42.1 The Specification of RSA

Theorem 42.1 *Let p and q be distinct prime numbers, let $m = pq$ and let $s = (p-1)(q-1)$. Let j and k be positive integers with the property that $j \equiv k \pmod{s}$. Then $x^j \equiv x^k \pmod{m}$ for all integers x.*

Proof We may order j and k so that $j \leq k$. Let x be an integer. Then either x is divisible by p or x is coprime to p. Let us first suppose that x is coprime to p. Then Fermat's Little Theorem (Theorem 41.17) ensures that $x^{p-1} \equiv 1 \pmod{p}$. But then $x^{r(p-1)} \equiv 1 \pmod{p}$ for all non-negative integers r (for if two integers are congruent modulo p, then so are the rth powers of those integers). In particular $x^{ns} \equiv 1 \pmod{p}$ for all non-negative integers n, where $s = (p-1)(q-1)$.

Now j and k are positive integers such that $j \leq k$ and $j \equiv k \pmod{s}$. It follows that there exists some non-negative integer n such that $k = ns + j$. But then $x^k = x^{ns}x^j$, and therefore $x^k \equiv x^j \pmod{p}$. We have thus shown that the congruence $x^j \equiv x^k \pmod{p}$ is satisfied whenever x is coprime to p. This congruence is also satisfied when x is divisible by p, since in that case both x^k and x^j are divisible by p and so are congruent to zero modulo p. We conclude that $x^j \equiv x^k \pmod{p}$ for all integers x. On interchanging the roles of the primes p and q we find that $x^j \equiv x^k \pmod{q}$ for all integers x. Therefore, given any integer x, the integers $x^k - x^j$ is divisible by both p and q. But p and q are distinct prime numbers, and are therefore coprime. It follows that $x^k - x^j$ must be divisible by the product m of p and q (see Proposition 41.15). Therefore every integer x satisfies the congruence $x^j \equiv x^k \pmod{m}$, as required. ∎

The RSA encryption scheme works as follows. In order to establish the necessary public and private keys, one first chooses two distinct large prime numbers p and q. Messages to be sent are to be represented by integers n satisfying $0 \leq n < m$, where $m = pq$. Let $s = (p-1)(q-1)$, and let e be any positive integer that is coprime to s. Then there exists a positive integer d such that $ed \equiv 1 \pmod{s}$ (see Lemma 41.12). Indeed there exist integers d and t such that $ed - st = 1$ (Corollary 41.3), and appropriate values for d and t may by found using the Euclidean algorithm. Moreover d and t may be chosen such that $d > 1$, for if d' and t' satisfy the equation $ed' - st' = 1$, and if $d = d' + ks$ and $t = t' + ke$ for some integer k, then $ed - st = 1$. Thus, once a positive integer e is chosen coprime to s, standard algorithms enable one to calculate a positive integer d such that $ed \equiv 1 \pmod{s}$.

Now suppose that p, q, m, s, e and d have been chosen such that p and q are distinct prime numbers, $m = pq$, $s = (p-1)(q-1)$, e and d are coprime to s and $ed \equiv 1 \pmod{s}$. Let

$$I = \{n \in \mathbb{Z} : 0 \leq n < m\}.$$

Then for each integer x belonging to the set I, there exists a unique integer $E(x)$ that belongs to I and satisfies the congruence $E(x) \equiv x^e \pmod{m}$. Similarly, for each integer y belonging to the set I, there exists a unique integer $D(y)$ that belongs to I and satisfies the congruence $D(y) \equiv y^d \pmod{m}$. Now it follows from standard properties of congruences (Lemma 41.9) that if y and z are integers, and if $y \equiv z \pmod{m}$, then $y^d \equiv z^d \pmod{m}$. It follows that $D(E(x)) \equiv D(x^e) \equiv x^{ed} \pmod{m}$ for all integers x belonging to I. But $ed \equiv 1 \pmod{s}$, where $s = (p-1)(q-1)$. It follows from Theorem 42.1 that $x^{ed} \equiv x \pmod{m}$. We conclude therefore that $D(E(x)) \equiv x \pmod{m}$ for all $x \in I$. But every congruence class modulo m is represented by a single integer in the set I. It follows that that $D(E(x)) = x$ for all $x \in I$.

On reversing the roles of the numbers e and d, we find that $E(D(y)) = y$ for all $y \in I$. Thus $E\colon I \to I$ is an invertible function whose inverse is $D\colon I \to I$.

On order to apply the RSA cryptographic method one determines integers p, q, m, s, e and d. The pair (m, e) of integers represents the *public key* and determines the encryption function $E\colon I \to I$. The pair (m, d) of integers represents the corresponding *private key* and determines the decryption function $D\colon I \to I$. The messages to be sent are represented as integers belonging to I, or perhaps as strings of such integers. If Alice publishes her public key (m, e), but keeps secret her private key (m, d), then Bob can send messages to Alice, encrypting them using the encryption function E determined by Alice's public key. When Alice receives the message from Bob, she can decrypt it using the decryption function D determined by her private key.

Note that if the value of the integer s is known, where $s = (p-1)(q-1)$, then a private key can easily be calculated by means of the Euclidean algorithm. Obviously once the values of p and q are known, then so are the values of m and s. Conversely if the values of m and s are known, then p and q can easily be determined, since these prime numbers are the roots of the polynomial $x^2 + (s - m - 1)x + m$. Thus knowledge of s corresponds to knowledge of the factorization of the composite number m as a product of prime numbers. There are known algorithms for factoring numbers as products of primes, but one can make sure that the primes p and q are chosen large enough to ensure that massive resources are required in order to factorize their product pq using known algorithms. The security of RSA also rests on the assumption that there is no method of decryption that requires less computational resources than are required for factorizing the product of the prime numbers determining the public key.

It remains to discuss whether it is in fact feasable to do the calculations involved in encrypting messages using RSA. Now, in order determine the value of $E(x)$ for any non-negative integer x less than m, one needs to determine the congruence class of x^e modulo m. Now e could be a very large number. However, in order to determine the congruence class of x^e modulo m, it is not necessary to determine the value of the integer x^e itself. For given any non-negative integer x less than m, we can determine a sequence $a_0, a_1, a_2, a_3, \ldots$ of non-negative integers less than m such that $a_0 = x$ and $a_{i+1} \equiv a_i^2 \pmod{m}$ for each non-negative integer i. Then $a_i \equiv x^{2^i}$ for all non-negative integers i. Any positive integer e may then be expressed in the form

$$e = e_0 + 2e_1 + 2^2 e_2 + 2^3 e_3 + \cdots$$

where e_i has the value 0 or 1 for each non-negative integer i. (These numbers e_i are of course the digits in the binary representation of the number e.)

Then x^e is then congruent to the product of those integers a_i for which $e_k = i$. The execution time required to calculate $E(x)$ by this method is therefore determined by the number of digits in the binary expansion of e, and is therefore bounded above by some constant multiple of $\log m$ (assuming that e has been chosen so that it is less than s, and thus less than m).

Moreover the execution time required by the Euclidean algorithm, when applied to natural numbers that are less than m is also bounded above by some constant multiple of $\log m$. For in order to apply the Euclidean algorithm, one is required to calculate a decreasing sequence $r_0, r_1, r_2, r_3, \ldots$ such that, for $k \leq 2$, the non-negative integer r_k is the remainder obtained on dividing r_{k-2} by r_{k-1} in integer arithmetic, and therefore satisfies the inequality $r_k \leq \frac{1}{2} r_{k-2}$. (To see this, consider separately what happens in the two cases when $r_{k-1} \leq \frac{1}{2} r_{k-2}$ and $r_{k-1} > \frac{1}{2} r_{k-2}$.)