CHAPTER 2

Modular Arithmetic

In studying the integers we have seen that is useful to write $a = qb + r$. Often we can solve problems by considering only the remainder, r. This throws away some of the information, but is useful because there are only finitely many remainders to consider. The study of the properties of the system of remainders is called *modular arithmetic.* It is an essential tool in number theory.

2.1. Definition of $\mathbb{Z}/n\mathbb{Z}$

In this section we give a careful treatment of the system called the integers modulo (or mod) n.

2.1.1 Definition Let a, $b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. We say [1]that a *is congruent to* b *modulo* n , written

$$a \equiv b \pmod{n}$$

if $n \mid (a - b)$.

2.1.2 Example

- ★ $23 \equiv 3 \pmod{10}$ since $10 \mid (23 - 3)$.
- ★ $23 \equiv 7 \pmod{8}$ since $8 \mid (23 - 7)$.
- ★ $10000 \equiv 4 \pmod{7}$ since $(10000 - 4) = 9996 = 1428 \cdot 7$.

Since any two integers are congruent mod 1, we usually require $n \geq 2$ from now on.

Congruence modulo n generalizes the notion of divisibility, since

$$a \equiv 0 \pmod{n} \iff n \mid a.$$

More generally, if $a = qn + r$ then $a \equiv r \pmod{n}$, since $n \mid (a - r)$.

2.1.3 Theorem Let $n > 1$ and let a, b, c, $d \in \mathbb{Z}$. Then

(a) If $a = b$ then $a \equiv b \pmod{n}$.
(b) $a \equiv a \pmod{n}$.
(c) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
(d) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.
(e) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

Proof (a) $a - b = 0$ so $n \mid (a - b)$.

(b) Follows from (a).

(c) If $n \mid (a - b)$ then $n \mid (b - a)$.

(d) If $n \mid (a - b)$ and $n \mid (b - c)$ then $n \mid ((a - b) + (b - c))$ so $n \mid (a - c)$.

(e) Suppose $n \mid (a - b)$ and $n \mid (c - d)$. Then $n \mid ((a - b) + (c - d))$ so $n \mid ((a + c) - (b + d))$, that is, $a + c \equiv b + d \pmod{n}$.

[1]We are viewing $\equiv \pmod{n}$ as a sort of weakened equality: given two integers, they either are or are not congruent mod n. In computer science it is common to talk of the "mod n" operator, thinking of it as a function of one argument, and writing $a \bmod n = r$ to mean $a \equiv r \pmod{n}$ with $r \in \{0, 1, \ldots, n - 1\}$.

For multiplication, we may write $a - b = sn$ for some $s \in \mathbb{Z}$, so $a = sn + b$. Similarly $c = tn + d$. So $ac = (sn + b)(tn + d) = n(stn + sd + bt) + bd$ and $n \mid (ac - bd)$. □

2.1.4 Example

- ★ $5 + 8 \equiv 1 \pmod{12}$.
- ★ $5 \cdot 8 = 40 \equiv 4 \pmod{12}$.
- ★ $5^3 = 25 \cdot 5 \equiv 1 \cdot 5 \equiv 5 \pmod{12}$.

Modular arithmetic is sometimes introduced using clocks. If we depart at 5 o'clock and our journey takes 8 hours, we arrive at 1 o'clock. Only the remainder mod 12 is used for time in hours.

2.1.5 Example Let f be a polynomial with integer coefficients. Suppose $a \equiv b \pmod{n}$. Then $f(a) \equiv f(b) \pmod{n}$.

Proof We make repeated use of Theorem 2.1.3. If $a \equiv b$ then $a^2 \equiv b^2$, and so $a^3 \equiv b^3$ etc. So $a^k \equiv b^k$ for each k. So if $f = c_k x^k + \cdots + c_1 x + c_0$ then $f(a) = c_k a^k + \cdots + c_1 a + c_0 \equiv c_k b^k + \cdots + c_1 b + c_0 = f(b)$. □

2.1.6 Definition Let $n \in \mathbb{N}$, $n \geq 2$. Let $a \in \mathbb{Z}$. The *congruence class* of a, denoted $[a]_n$ or $[a]$ is the set of all integers congruent to a mod n:

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}.$$

Any element of $[a]$ is called a *representative* for the congruence class $[a]$.

We write $[a]$ instead of $[a]_n$ unless we are working modulo two different bases.

Note that the congruence class $[a]$ is a *set* of integers.

2.1.7 Example Let $n = 2$. Then

- $[0] = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$, the set of even integers.
- $[1] = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$, the set of odd integers.

Note that $[0] = [2] = [4]$, $[1] = [3] = [5]$ and so on, so there are just these two congruence classes. We say that 0 is a representative for $[0]$, 2 is another representative for $[0]$ and so on. Each congruence class has infinitely many representatives.

2.1.8 Example Let $n = 4$. Then

- $[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$.
- $[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$.
- $[2] = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$.
- $[3] = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$.

And $[4] = [0]$, $[5] = [1]$ and so on, so there are just these four congruence classes. Here 0 is a representative for $[0]$, 4 is another representative for $[0]$ and so on.

2.1.9 Theorem $a \equiv c \pmod{n}$ iff $[a] = [c]$.

Proof $\Longrightarrow$ Suppose $a \equiv c \pmod{n}$. Let $b \in [a]$. Then $b \equiv a \pmod{n}$. But $a \equiv c \pmod{n}$, so $b \equiv c \pmod{n}$ (Theorem 2.1.3). Hence $b \in [c]$. Since $b \in [a]$ was arbitrary, $[a] \subseteq [c]$. A similar argument shows that if $b \in [c]$ then $b \in [a]$, so $[c] \subseteq [a]$. Thus $[a] = [c]$.

$\Longleftarrow$ Suppose $[a] = [c]$. Since $a \equiv a \pmod{n}$ we know that $a \in [a] = [c]$, so $a \equiv c \pmod{n}$. □

2.1.10 Corollary Any two congruence classes mod n are either equal or disjoint.

Proof Let $[a]$ and $[c]$ be two congruence classes. If they are disjoint there is nothing to prove. So assume there is an element b in their intersection. Then by definition of congruence class, $b \equiv a$ and $b \equiv c \pmod{n}$, so $a \equiv c \pmod{n}$ so $[a] = [c]$ by the previous theorem. □

This means that the congruence classes mod n partition the integers into disjoint blocks. We saw this above for the integers mod 4: there are only four congruence classes, [0], [1], [2], [3]. This is true in general.

2.1.11 Theorem There are exactly n congruence classes modulo n, namely $[0]$, $[1]$, $\ldots$, $[n-1]$.

Proof We first show that these classes are all distinct. Suppose $0 \le r < s < n$. Then $0 < s - r < n$. There is no integer multiple of n in the interval $(0, n)$, so $n \nmid (s-r)$, so $r \not\equiv s \pmod{n}$. Then by Theorem 2.1.9, $[r] \neq [s]$. So no two of $[0]$, $[1]$,$\ldots$ $[n-1]$ are equal.

Next we show that every congruence class is equal to one of these listed. Let $a \in \mathbb{Z}$. By the Division Algorithm we may write $a = qn + r$ with $r = 0$ or 1 or $\ldots$ or $n-1$. Now $a \equiv r \pmod{n}$ (since $a - r = qn$). By Theorem 2.1.9, $[a] = [r]$ with $r = 0$ or 1 or $\ldots$ or $n-1$. □

2.1.12 Definition The set of congruence classes mod n is called the set of *integers modulo n,* and denoted $\mathbb{Z}/n\mathbb{Z}$.

Many authors write $\mathbb{Z}_n$ for $\mathbb{Z}/n\mathbb{Z}$, but this conflicts with other notation in number theory. (Some people just write $\mathbb{Z}/n$.)

Warning: the elements of $\mathbb{Z}/n\mathbb{Z}$ are congruence classes, *not* integers. Each element is a *set* of integers. For example, $\mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\}$. This is *not* a subset of $\mathbb{Z}$.

Furthermore, according to Theorem 2.1.9 each congruence class has many different names. For example $[0] = [4] = [-12]$ in $\mathbb{Z}/4\mathbb{Z}$. It is perfectly correct to write $\mathbb{Z}/4\mathbb{Z} = \{[-12], [17], [10], [7]\}$: $[-12] = \{\ldots, -16, -12, -8, -4, 0, 4, \ldots\} = [0]$. This follows since $-12 \equiv 0 \pmod{4}$. Similarly $17 \equiv 1 \pmod{4}$, so $[17] = [1]$ etc.

However, we do have the following important function:

2.1.13 Definition Define a function $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by

$$\pi(a) = [a].$$

The function π is called the *reduction mod n function.*

2.2. Defining Operations in $\mathbb{Z}/n\mathbb{Z}$

The integers mod n are clearly closely related to the integers $\mathbb{Z}$. It is natural to wonder if we can add and multiply in $\mathbb{Z}/n\mathbb{Z}$. We can, but it takes some care.

Suppose $[a]$, $[b] \in \mathbb{Z}/n\mathbb{Z}$. How can we define the sum of these two classes? A natural idea is to try the following:

$$[a] \oplus [b] = [a + b]. \tag{2.2.1}$$

Here $\oplus$ is a new operation we are defining: an addition on the set $\mathbb{Z}/n\mathbb{Z}$. It is *not* the usual addition $+$ of integers. In words: to add $[a]$ and $[b]$, find the class containing $a + b$.

2.2.1 Example In $\mathbb{Z}/5\mathbb{Z}$, $[2] \oplus [4] = [2 + 4] = [6] = [1]$. $[3] \oplus [2] = [5] = [0]$.

However there is a serious difficulty. The elements of $\mathbb{Z}/n\mathbb{Z}$ have many different names, and our addition rule (equation 2.2.1) seems to depend on the particular name chosen. Do we get the same answer, no matter which name we use?

2.2.2 Example In $\mathbb{Z}/5\mathbb{Z}$, $[2] = [7]$ and $[4] = [9]$. Is $[2] \oplus [4] = [7] \oplus [9]$? Above, $[2] \oplus [4] = [1]$. $[7] \oplus [9] = [16] = [1]$, so we get the same answer in this case.

This is always the case:

2.2.3 Theorem $\oplus$ is well defined on $\mathbb{Z}/n\mathbb{Z}$. That is, it does not depend on the particular names of the congruence classes chosen in equation 2.2.1.

Proof Let $[a], [c] \in \mathbb{Z}/n\mathbb{Z}$. We must show that if $[a] = [b]$ and $[c] = [d]$ then $[a] \oplus [c] = [b] \oplus [d]$.

Now $[a] = [b]$ implies $a \equiv b \pmod{n}$ (Theorem 2.1.9) and similarly $[c] = [d]$ implies $c \equiv d \pmod{n}$. Thus $a + c \equiv b + d \pmod{n}$ by Theorem 2.1.3, so $[a + c] = [b + d]$. Hence $[a] \oplus [c] = [b] \oplus [d]$. □

2.2.4 Example Here is the complete addition table mod 3:

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

We can define multiplication mod n in a similar way.

2.2.5 Definition Define multiplication $\odot$ on $\mathbb{Z}/n\mathbb{Z}$ by

$$[a] \odot [b] = [ab].$$

2.2.6 Theorem $\odot$ is well defined on $\mathbb{Z}/n\mathbb{Z}$.

Proof Exercise. We have to show that if $[a] = [b]$ and $[c] = [d]$ then $[a] \odot [c] = [b] \odot [d]$. The Theorems needed are 2.1.9 and 2.1.3. □

2.2.7 Example Here is the complete multiplication table mod 3:

$\odot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

In fact $\oplus$ and $\odot$ in $\mathbb{Z}/n\mathbb{Z}$ behave very much like addition and multiplication of integers:

2.2.8 Theorem For any classes $[a]$, $[b]$, $[c] \in \mathbb{Z}/n\mathbb{Z}$

(a) $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$

(b) $[a] \oplus [0] = [a] = [0] \oplus [a]$.

(c) $[a] \oplus [-a] = [0] = [-a] \oplus [a]$.

(d) $[a] \oplus [b] = [b] \oplus [a]$.

(e) $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$

(f) $[a] \odot [1] = [a] = [1] \odot [a]$.

(g) $[a] \odot [b] = [b] \odot [a]$.

(h) $[a] \odot ([b] \oplus [c]) = ([a] \odot [b]) \oplus ([a] \odot [c])$.

(i) $([a] \oplus [b]) \odot [c] = ([a] \odot [c]) \oplus ([b] \odot [c])$.

Proof Each property follows from the analogous property about integers. For example to prove (d):

$[a] \oplus [b] = [a + b] = [b + a]$ (since $a + b = b + a$ for integers a and b), and $[b + a] = [b] \oplus [a]$.

The other properties are just as simple and are left as exercises.
qed

Not every algebraic property of the integers extends to $\mathbb{Z}/n\mathbb{Z}$.

2.2.9 Example

- ★ In $\mathbb{Z}/6\mathbb{Z}$ we have $[2] \odot [3] = [6] = [0]$. So two non-zero elements can multiply to give $[0]$.
- ★ In $\mathbb{Z}/6\mathbb{Z}$, $[2] \odot [1] = [2] = [2] \odot [4]$ but $[1] \neq [4]$. So cancellation fails: $ab = ac$ does not imply $b = c$ (even if $a \neq [0]$).

We shall come back to these examples in the algebra section.

2.3. New notation for $\mathbb{Z}/n\mathbb{Z}$

So far we have been very careful to distinguish between integers and elements of $\mathbb{Z}/n\mathbb{Z}$ (which are *sets* of integers). We have defined addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$, and seen that we have to check carefully that these definitions make sense.

However, mathematicians are lazy, and often abuse notation. We adopt this common practice.

2.3.1 Definition From now on when working mod n, we write a to mean the congruence class $[a]$. We write $a + b$ instead of $[a] \oplus [b]$ and ab instead of $[a] \odot [b]$. We also write $a - b$ for $[a] \oplus [-b]$. We call $[0]$ the *zero element* .

Nonetheless we should always bear in mind the distinction between $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$. For example, mod 5 we have $1 = 6$, which is not true in $\mathbb{Z}$. We have $2 + 3 = 0$ which is also false in $\mathbb{Z}$. To mitigate this confusion, we continue to write $\equiv \pmod{n}$ where convenient.

If there is any occasion where the context does not make clear if we are working in $\mathbb{Z}$ or in $\mathbb{Z}/n\mathbb{Z}$, we revert to the $[a]$ notation.

Finally, we occasionally write $a \pmod{n}$ to mean the representative r of the congruence class $[a]$ with $0 \leq r < n$. This notation is common in computer science etc.

We give some further examples of calculations mod n. One great advantage of $\mathbb{Z}/n\mathbb{Z}$ is that it is finite, so we can simply test all possibilities.

2.3.2 Example For all $n \in \mathbb{Z}$, $n^2 \equiv 0$ or $1 \pmod{4}$. (Compare Example 1.4.4).

Proof We know that $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$. So $n^2 \equiv 0^2$, 1^2, 2^2 or 3^2. But $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 = 4 \equiv 0$, and $3^2 = 9 \equiv 1 \pmod{4}$. □

2.3.3 Example For all $n \in \mathbb{Z}$, $7 \mid n^3$ or $7 \mid n^3 \pm 1$.

Proof The 7 congruences classes mod 7 may be represented by $\{-3, -2, -1, 0, 1, 2, 3\}$ since $4 \equiv -3$, $5 \equiv -2$, $6 \equiv -1$.

n	-3	-2	-1	0	1	2	3
n^3	$-27 \equiv 1$	$-8 \equiv -1$	-1	0	1	$8 \equiv 1$	$27 \equiv -1$

Thus $n^3 \equiv 0$ or $\pm 1 \pmod{7}$ for every n. □

2.3.4 Example Prove that the equation $x^3 + 10000 = y^3$ has no solutions in integers x, y.

Proof If $x^3 + 10000 = y^3$ then $x^3 + 10000 \equiv y^3 \pmod{7}$ (by Theorem 2.1.3(1)). Since $10000 \equiv 4 \pmod{7}$,

$$x^3 + 4 \equiv y^3 \pmod{7}.$$

But $x^3 \equiv -1, 0$, or $1 \pmod{7}$ by previous example, so $x^3 + 4 \equiv 3, 4$ or $5 \pmod{7}$, while $y^3 \equiv -1, 0$, or $1 \pmod{7}$ contradiction. □

This example illustrates one of the uses of modular arithmetic. Modulo n there are only ever finitely many possible cases, and we can (in principle) check them all.

2.3.5 Example What is the last decimal digit of 3^{2010}?

Solution: We note that $3^1 \equiv 3 \pmod{10}$, $3^2 \equiv 9$, $3^3 \equiv 7$ and $3^4 \equiv 1 \pmod{10}$. So

$$3^{2010} = 3^{4\cdot 502+2} = (3^4)^{502} \cdot 3^2 \equiv 1^{502} \cdot 9 = 9 \pmod{10}.$$

So the last digit is 9. □

16 Exercise

(a) Prove that $6 \mid a(a^2+11)$ for any integer a.
(b) Prove that if a and b are odd then $a^2 - b^2$ is a multiple of 8.

17 Exercise

Find all solutions of $x^2 + y^2 = z^2$ with x, y, $z \in \mathbb{N}$. (Pythagorean triples.)

(a) Recall from Exercise 11 that n is a square iff every exponent occurring in the factorization of n is even. Using this, prove that if $d^2 \mid m^2$ then $d \mid m$.
(b) Hence prove that if $\gcd(u, v) = 1$ and uv is a square then u and v are squares.
(c) Show that if d divides any two of x, y, z then it divides the third.
(d) Let $d = \gcd(x, y, z)$. Let $X = x/d$, $Y = y/d$, $Z = z/d$. Show that $X^2 + Y^2 = Z^2$ with $\gcd(X, Y) = \gcd(X, Z) = \gcd(Y, Z) = 1$.
(e) Show that one of X and Y must be even and one must be odd, and that Z must be odd. Hint: work mod 4.
(f) Without loss of generality, let Y be even, say $Y = 2c$ and let X and Z be odd. Let $u = (X+Z)/2$, $v = (Z-X)/2$. Show that $uv = c^2$ and $\gcd(u, v) = 1$.
(g) Conclude that $u = a^2$ and $v = b^2$ for some a, $b \in \mathbb{Z}$.
(h) Hence show that $X = a^2 - b^2$, $Y = 2ab$ and $Z = a^2 + b^2$.
(i) Obtain a Pythagorean triple with 2004 as one of the sides.

2.4. Powers in $\mathbb{Z}/n\mathbb{Z}$: Repeated Squaring

We can calculate powers in $\mathbb{Z}/n\mathbb{Z}$ rapidly using *repeated squaring.*

2.4.1 Example Show that $11 \mid (3^{32} + 2)$.

Solution: We repeatedly square mod 11.

$$\begin{array}{lllllll} & 3^2 & \equiv & 9 & & & \\ 3^4 & = (3^2)^2 & \equiv & 9^2 & \equiv & 4 & \pmod{11} \\ 3^8 & = (3^4)^2 & \equiv & 4^2 & \equiv & 5 & \pmod{11} \\ 3^{16} & = (3^8)^2 & \equiv & 5^2 & \equiv & 3 & \pmod{11} \\ 3^{32} & = (3^{16})^2 & \equiv & 3^2 & \equiv & 9 & \pmod{11} \end{array}$$

So $3^{32} + 2 \equiv 0 \pmod{11}$ so $11 \mid (3^{32} + 2)$.

We calculate 3^{32} using only 5 multiplications (squarings), instead of 32.

2.4.2 Example Find the last 2 decimal digits of 2^{100}.

Solution: We work in $\mathbb{Z}/100\mathbb{Z}$.

$$\begin{array}{lllllll} & 2^2 & \equiv & 4 & & & \\ 2^4 & = (2^2)^2 & \equiv & 4^2 & \equiv & 16 & \pmod{100} \\ 2^8 & = (2^4)^2 & \equiv & 16^2 & \equiv & 56 & \pmod{100} \\ 2^{16} & = (2^8)^2 & \equiv & 56^2 & \equiv & 36 & \pmod{100} \\ 2^{32} & = (2^{16})^2 & \equiv & 36^2 & \equiv & -4 & \pmod{100} \\ 2^{64} & = (2^{32})^2 & \equiv & (-4)^2 & \equiv & 16 & \pmod{100} \end{array}$$

Now $100 = 64 + 32 + 4$, so

$$2^{100} = 2^{64} \cdot 2^{32} \cdot 2^4 \equiv 16 \cdot (-4) \cdot 16 \equiv 76 \pmod{100}.$$

So $2^{100} \equiv 76 \pmod{100}$. This calculation required only $6 + 3 = 9$ multiplications instead of 100.

In general to calculate $a^N \pmod{n}$ we need one or two multiplications for each power of 2 below N, for a total of at most $2\log_2(N)$ multiplications or $c\log(N)$ multiplications, for some constant c.

2.4.3 Theorem It is possible to calculate $a^N \pmod{n}$ using only $c\log(N)$ multiplications, for some constant c. □

This means it is feasible to calculate a^N, even if the exponent N has thousands of digits.

2.4.4 Example Suppose a computer does 1 billion mod n multiplications per second. Suppose we want to calculate

$$a^{100,000,000,000,000,000,000} \pmod{n}.$$

So we want $a^N \pmod{n}$ with $N = 10^{20}$. Multiplying a by itself 10^{20} times would take 10^{20} operations, or about 3000 years. Using repeated squaring would take only about $2\log_2(10^{20})$ operations or about 0.1 microseconds (millionths of a second).

2.4.5 Algorithm [Powers mod n] Given $x \in \mathbb{Z}$, $n, N \in \mathbb{N}$ with $n \geq 2$ this algorithm returns $x^N \mod n$. The algorithm is recursive:

$$\text{Power}(x, n) = \begin{cases} \text{Return } x, & \text{if } n = 1 \\ \text{Return Power}\left(x, \frac{n}{2}\right), & \text{if } n \text{ is even} \\ \text{Return } x \cdot \text{Power}\left(x, \frac{(n-1)}{2}\right), & \text{if } n \text{ is odd} \end{cases}$$

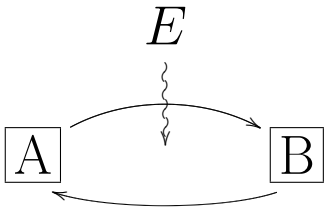
18 Exercise Calculate $2^{341} \pmod{340}$.

19 Exercise Find the smallest integer larger than 11^{104} that is exactly divisible by 17.

2.5. Application: Diffie-Hellman Key Exchange

Many encryption schemes assume that the users know a secret key (usually a number). Anyone possessing the key can decrypt messages.

How can Alice and Bob establish a secret key in the first place? Suppose they cannot meet in person. Phones can be tapped, email read enroute etc.



Suppose an eavesdropper Eve can read every message that passes between A and B. It is still possible for A and B to set up a secret key, right under E's nose. The algorithm is based on the following observation:

- Given a and N, it is easy to calculate $a^N \pmod{n}$.
- Given $a^N \pmod{n}$ and a it is very hard to find N.

2.5.1 Definition The task of finding N given $a^N \pmod{n}$ is called the *discrete logarithm problem* .

Note: over $\mathbb{R}$ if $a^N = b$ then $N = \log_a(b)$, hence the name. Of course the log function is not defined mod n.

2.5.2 Example If $2^N \equiv 3 \pmod{11}$, find N.

Solution: We just have to try all the possibilities in turn.

N	1	2	3	4	5	6	7	8
2^N	2	4	8	5	10	9	7	3

So $N = 8$.

If n and N are about 10^{100} in size then this is a hopeless task since potentially we would have to check all 10^{100} possible N ...

2.5.3 Algorithm [The Diffie-Hellman key exchange algorithm]

(a) A and B publicly choose a large prime number p and base a.
(b) A secretly chooses a number s, and sends $a^s \pmod{p}$ to B.
(c) B secretly chooses a number t, and sends $a^t \pmod{p}$ to A.
(d) A secretly calculates $k = (a^t)^s \pmod{p}$. B secretly calculates $k = (a^s)^t \pmod{p}$. Let k be the secret key.

A and B never reveal s, t or k to anyone else.

E can see a^s and $a^t \pmod{p}$ but cannot efficiently find the discrete logarithms s and t, so she cannot find $k = a^{st}$.

(E can always find k given enough time. But if p is chosen large enough: say $p > 10^{100}$ then the running time is expected to be trillions of trillions of years, so the key is effectively safe.)

2.5.4 Example Example: Suppose $a = 2$, $p = 11$. Suppose A choose $s = 4$ and B chooses $t = 8$. Calculate the secret key.

Solution:

- A sends $2^4 \equiv 5 \pmod{11}$ to B.
- B sends $2^8 \equiv 3 \pmod{11}$ to A.
- A receives 3 from B and calculates $k = 3^s = 3^4 \equiv 4 \pmod{11}$.
- B receives 5 from A and calculates $k = 5^t = 5^8 \equiv 4 \pmod{11}$.
- This establishes the secret key $k = 4$ for A and B to use.

The eavesdropper E sees $5 \equiv 2^s$ and $3 \equiv 2^t$ go by, but she is not able to calculate s and t quickly. So she cannot find k.

(Of course in this example the numbers are so small that E can easily find s and t by trial and error. In practice s and t would be at least 100 digits long.)

2.6. Inverses in $\mathbb{Z}/n\mathbb{Z}$

We have seen how to add, subtract and multiply mod n. What about division? Since dividing is the same as multiplying by the inverse (reciprocal), we need to investigate the existence of inverses mod n.

2.6.1 Definition Let $a \in \mathbb{Z}/n\mathbb{Z}$. A solution $x \in \mathbb{Z}/n\mathbb{Z}$ of the equation

$$ax \equiv 1 \pmod{n}$$

is called an *inverse* of a mod n, and denoted a^{-1}.

2.6.2 Example

- ★ $3 \cdot 4 \equiv 1 \pmod{11}$, so 4 is an inverse of 3 mod 11.
- ★ $5 \cdot 5 \equiv 1 \pmod{12}$ so 5 is its own inverse, mod 12.
- ★ $2x \equiv 1 \pmod{10}$ has no solution. *Proof* If $2x \equiv 1 \pmod{10}$ then $10 \mid (2x-1)$. But $2x-1$ is odd, so is not divisible by 10. So 2 is not invertible mod 10.

Which classes are invertible, mod n? The answer is those a with $\gcd(a,n) = 1$. However, we have to be careful that our abuse of notation does not lead us astray.

2.6.3 Theorem If $[a] = [c]$ in $\mathbb{Z}/n\mathbb{Z}$ then $\gcd(a,n) = \gcd(c,n)$.

Proof If $[a] = [c]$ then $a \equiv c \pmod{n}$ by Theorem 2.1.9. Let $a - c = qn$, for some integer q, so $a = qn + c$. Then $\gcd(a,n) = \gcd(c,n)$ by Theorem 1.5.1. □

So the statement $\gcd(a,n) = 1$ makes sense for congruence classes mod n.

2.6.4 Theorem a is invertible mod n iff $\gcd(a,n) = 1$.

Proof By definition, a is invertible mod n iff there exists an integer x with $ax \equiv 1 \pmod{n}$. This is true iff there also exists an integer y with

$$ax + ny = 1.$$

But this equation is solvable in x and y iff $\gcd(a,n) = 1$, by Theorem 1.6.5. □

Note: this is an example of an iff proof where we can do both directions at once, since each step is a statement $P \iff Q$.

2.6.5 Corollary Let p be a prime number. Then every non-zero element of $\mathbb{Z}/p\mathbb{Z}$ is invertible.

Proof If $a \in \mathbb{Z}/p\mathbb{Z}$ is non-zero then $a \not\equiv 0 \pmod{p}$, so $p \nmid a$. Since the only factors of p are 1 and p, this means $\gcd(a,p) = 1$, and a is invertible. □

This says that we can "divide by" any non-zero element in $\mathbb{Z}/p\mathbb{Z}$. In this respect $\mathbb{Z}/p\mathbb{Z}$ is similar to the real numbers. We shall discuss this further later in the course.

2.6.6 Example Which numbers are invertible mod 12?

Solution: The classes mod 12 are 0, 1, ..., 11. A class a is invertible mod 12 iff $\gcd(a,12) = 1$ by Theorem 2.6.4. Testing in turn, $\gcd(0,12) = 12 > 1$, $\gcd(2,12) = 2 > 1$, $\gcd(3,12) > 1$ etc. So a is invertible mod 12 iff $a \equiv 1, 5, 7, 11 \pmod{12}$. Thus there are 4 invertible elements mod 12.

2.6.7 Theorem Let $n \in \mathbb{N}$, $n \geq 2$, and let $a \in \mathbb{Z}$.

(a) If a is invertible, then its inverse is unique mod n.
(b) If a is invertible so is a^{-1}, and $(a^{-1})^{-1} \equiv a$.

Proof (a Suppose b and c are both inverses of a mod n. Then $ab \equiv ac \equiv 1 \pmod{n}$. So $a(b-c) \equiv 0 \pmod{n}$ which says that $n \mid a(b-c)$. Now if a is invertible, $\gcd(n,a) = 1$ by Theorem 2.6.4, so $n \mid (b-c)$ by Theorem 1.7.1. Thus $b \equiv c \pmod{n}$.

(b) If a is invertible then $aa^{-1} \equiv a^{-1}a \equiv 1 \pmod{n}$. This says that a is the inverse of a^{-1}. □

This result means we can talk of *the* inverse of a, not just an inverse.

2.6.8 Theorem Let $n \in \mathbb{N}$, $n \geq 2$, and let $a, b \in \mathbb{Z}$. If $\gcd(a,n) = 1$ then the congruence equation

$$ax \equiv b \pmod{n}$$

has a unique solution x mod n.

Proof Take $x = a^{-1}b$. Then $ax = aa^{-1}b \equiv 1 \cdot b = b \pmod{n}$, so the equation has a solution.

If x_1 and x_2 are two solutions then $ax_1 \equiv ax_2$, so multiplying by a^{-1} on each side, $x_1 \equiv x_2$, so the solution is unique. □

As we have seen, $ax \equiv b \pmod{n}$ may not be solvable if $\gcd(a, n) \neq 1$. Or it may be solvable with more than one solution:

2.6.9 Example The equation $3x \equiv 0 \pmod{6}$ has solutions $x \equiv 0, 2$ or $4 \pmod{6}$. Note that $ax_1 \equiv ax_2$ does not imply $x_1 \equiv x_2$ in this case.

2.6.10 Theorem $a^{-1}a^k \equiv a^{k-1} \pmod{n}$. This motivates the negative power notation for inverses.

Proof Exercise. □

20 Exercise Prove theorem 2.6.10.

How do we actually calculate inverses mod n? Let $n \in \mathbb{N}$ with $n \geq 2$ and let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then a is invertible, with a unique inverse mod n (Theorems 2.6.4, 2.6.7). To calculate a^{-1}, we apply Theorem 1.6.5 to write

$$nx + ay = 1$$

for some integers x, y. Reducing this equation mod n,

$$ay \equiv 1 \pmod{n}$$

so y is the desired a^{-1}. (The value of x is irrelevant.)

2.6.11 Algorithm [Inverses Mod n] To calculate a^{-1} mod n, find x and y with $nx + ay = 1$, using the Extended Euclidean Algorithm. Then $y \equiv a^{-1} \pmod{n}$.

2.6.12 Example Calculate $11^{-1} \pmod{80}$.

Solution: We want to write $80x + 11y = 1$.

q	r	x	y
	80	1	0
7	11	0	1
3	3	1	−7
1	2	−3	22
2	1	4	−29
	0		

So $80 \cdot (4) + 11 \cdot (-29) = 1$, so $1 \equiv (-29) \cdot 11 \pmod{80}$, so $11^{-1} \equiv -29 \equiv 51 \pmod{80}$.

Check: $11 \cdot 51 = 561 = 7 \cdot 80 + 1 \equiv 1 \pmod{80}$. (Note: there was actually no need for the x column in this calculation.)

This may seem like quite a lot of calculation, but in fact it is extremely efficient, even for very large numbers.

2.6.13 Example Solve the congruence equation $11x \equiv 4 \pmod{80}$.

Solution: If $11x \equiv 4 \pmod{80}$ then $x \equiv 11^{-1} \cdot 4 \equiv 51 \cdot 4 \equiv 44 \pmod{80}$. Check: $11 \cdot 44 = 484 \equiv 4 \pmod{80}$.

21 Exercise Calculate $14^{-1} \pmod{23}$. Hence solve the congruence $14x \equiv 11 \pmod{23}$.

2.7. The Euler φ Function

Recall that an integer a is invertible mod n iff $\gcd(a, n) = 1$.

2.7.1 Definition Define a function $\varphi\colon \mathbb{N} \to \mathbb{N}$ by

$$\varphi(n) = \text{ The number of } a \text{ with } 1 \le a \le n \text{ and } \gcd(a, n) = 1.$$

This is called the *Euler φ function* . Equivalently, $\varphi(n)$ is the number of invertible elements modulo n.

2.7.2 Example The numbers a with $1 \le a \le 12$ and a relatively prime to 12 are 1, 5, 7 and 11, so $\varphi(12) = 4$. Note that 1, 5, 7, 11 are exactly the invertible elements modulo 12 (Example 2.6.6).

n	Invertible elements mod n	$\varphi(n)$
2	1	1
3	1, 2	2
4	1, 3	2
5	1, 2, 3, 4	4
6	1, 5	2
7	1, 2, 3, 4, 5, 6	6
8	1, 3, 5, 7	4
9	1, 2, 4, 5, 7, 8	6
10	1, 3, 7, 9	4
12	1, 5, 7, 11	4

2.7.3 Theorem Let p be a prime number and $k \in \mathbb{N}$. Then

$$\varphi(p^k) = p^{k-1}(p-1).$$

Proof $\varphi(p^k) = p^k$ minus the number of a with $1 \le a \le p^k$ and $\gcd(a, p^k) > 1$.

Now $\gcd(a, p^k) > 1$ implies a and p^k share a common factor, hence a common prime factor, which must be p. Conversely if $p \mid a$ then $\gcd(a, p^k) > 1$. So the numbers with $\gcd(a, p^k) > 1$ are precisely the multiples of p, and there are $p^k/p = p^{k-1}$ of these in the specified range. So $\varphi(p^k) = p^k - p^{k-1}$. □

2.7.4 Theorem If $\gcd(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof Deferred until we develop some more algebra. □

Warning: Theorem 2.7.4 is false without the gcd assumption: $\varphi(mn) \ne \varphi(m)\varphi(n)$ in general. For example $\varphi(9) = 3^2 - 3 = 6 \ne \varphi(3)\varphi(3) = 4$.

Theorems 2.7.3 and 2.7.4 gives us a formula for calculating $\varphi(n)$ for any n. If $n = p_1^{a_1} \cdots p_k^{a_k}$ where the p_i are distinct primes then

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_k^{a_k}) \\ &= (p_1^{a_1-1})(p_1 - 1)(p_2^{a_2-1})(p_2 - 1) \cdots (p_k^{a_k-1})(p_k - 1) \end{aligned}$$

2.7.5 Example Calculate $\varphi(540)$.

Solution:

$$\begin{aligned} 540 &= 2^2 \cdot 3^3 \cdot 5 \\ \varphi(540) &= \varphi(2^2)\varphi(3^3)\varphi(5) \\ &= 2(2-1)3^2(3-1)(5-1) = 144 \end{aligned}$$

22 Exercise Calculate $\varphi(n)$ for $1 \le n \le 20$. Calculate $\varphi(2010)$.

23 Exercise Prove that $\varphi(n)$ is even for all $n \geq 3$. Prove that $\varphi(n) = 14$ has no solution, and 14 is the smallest even natural number with this property. Find all n with $\varphi(n) = 6$.

24 Exercise Show that $\varphi(n^2) = n\varphi(n)$. Show that if $m \mid n$ then $\varphi(m) \mid \varphi(n)$.

25 Exercise Show that

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p}).$$

where p is prime and $\prod$ denotes the product.

2.8. The Chinese Remainder Theorem

We have seen how to solve linear congruences $ax \equiv b \pmod{m}$. What about simultaneous systems of congruences? Consider the following problem. Let $m_1, \ldots, m_n \in \mathbb{N}$, and let $a_i \in \mathbb{Z}$ with $1 \leq i \leq n$. Can we find an integer x that *simultaneously* satisfies

$$x \equiv a_i \pmod{m_i}, \qquad 1 \leq i \leq n?$$

2.8.1 Example The system

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 1 \pmod{2} \end{aligned}$$

clearly is inconsistent. No integer x can be both 0 and 1 mod 2.

2.8.2 Example The system

$$\begin{aligned} x &\equiv 4 \pmod{7} \\ x &\equiv 9 \pmod{11} \\ x &\equiv 3 \pmod{13} \end{aligned}$$

is solvable: $x = 900$ is a solution.

A condition that guarantees consistency of a simultaneous system is that the moduli be relatively prime in pairs. (That is, no two of them share a factor.)

2.8.3 Theorem [Chinese Remainder Theorem] Let $m_1, \ldots, m_n$ be pairwise relatively prime positive integers. Let $a_i \in \mathbb{Z}$, $1 \leq i \leq n$. Then any simultaneous system of congruences

$$x \equiv a_i \pmod{m_i} \qquad i = 1, 2, \ldots n$$

is solvable. Moreover the solution is unique modulo $m_1 m_2 \cdots m_n$.

Proof We give a constructive proof. The idea is to find a number e_1 that is 0 mod m_2, m_3, …, m_n but $e_1 \equiv a_1 \pmod{m_1}$. Similarly find an e_2 that is 0 mod m_1, m_3, m_4 …, m_n but is a_2 mod m_2. Etc. The desired x will then be $e_1 + e_2 + \cdots + e_n$. It is easy to find a number that is 0 mod m_i for $i = 2, 3, \ldots$. Just take $m_2 m_3 \cdots m_n$. This will not be 0 mod m_1 (see below) so we can scale it to make it a_1, by first multiplying by its inverse mod m_1 and then multiplying by a_1.

The details are as follows: Let

$$M = \prod_j m_j \qquad M_i = \prod_{j \neq i} m_j = M/m_i.$$

Then $\gcd(m_i, M_i) = 1$ because M_i is a product of numbers relatively prime to m_i (theorem 1.8.4). So let N_i be an integer with

$$M_i N_i \equiv 1 \pmod{m_i}.$$

Finally let

$$x = \sum a_i M_i N_i.$$

If we reduce x mod m_i, every term in the sum is 0 except the ith because m_i divides every other M_j. So $x \equiv a_i M_i N_i \equiv a_i \cdot 1 = a_i \pmod{m_i}$ as required. This proves existence.

If y is another solution of the system then $x - y \equiv 0 \pmod{m_i}$ for each i, so $m_i \mid (x-y)$. But the m_i are relatively prime, so $m_1 \cdots m_n \mid (x-y)$ by Theorem 1.7.6, so $x \equiv y \pmod{m_1 \cdots m_n}$. □

2.8.4 Example Solve the system

$$\begin{aligned} x &\equiv 4 \pmod 7 \\ x &\equiv 9 \pmod{11} \\ x &\equiv 3 \pmod{13} \end{aligned}$$

Solution: $m_1 = 7$, $m_2 = 11$, $m_3 = 13$.

$$M_1 = 11 \cdot 13, \quad M_2 = 7 \cdot 13, \quad M_3 = 7 \cdot 11.$$

Then

$$M_1 \equiv 3 \pmod 7, \quad M_2 \equiv 3 \pmod{11}, \quad M_3 \equiv -1 \pmod{13}.$$

Thus we can take

$$N_1 = 5, \quad N_2 = 4, \quad N_3 \equiv -1 \pmod{13}.$$

So

$$\begin{aligned} x &= a_1 M_1 N_1 + a_2 M_2 N_2 + a_3 M_3 N_3 \\ &= 4 \cdot (11 \cdot 13) \cdot 5 + 9 \cdot (7 \cdot 13) \cdot 4 + 3 \cdot (7 \cdot 11) \cdot (-1) \\ &= 5905 \\ &\equiv 900 \pmod{7 \cdot 11 \cdot 13}. \end{aligned}$$

According to legend, soldiers at drill in China used to line up in groups of various sizes. Suppose they line up in groups of 7. The number of left over (remaining) soldiers could then easily be counted. Next they could line up in 11's and then in 13's. If the remainders were 4, 9, 3 respectively, then the total number n of soldiers is determined mod $7 \cdot 11 \cdot 13 = 1001$ by solving the system (2.8.2). As above, a solution is $n = 900$. Solving the system of congruences is much faster than counting all 900 soldiers. Hence the name of the Theorem.

The main use of the CRT is to break a problem mod n up into one or more problems mod p^k, and then to reassemble the pieces to solve the original problem.

2.8.5 Example Solve the equation $x^2 + 1 \equiv 0 \pmod{85}$.

Solution: At first this seems to have nothing to do with the CRT. However any solution must satisfy $85 \mid (x^2+1)$. Since $85 = 5 \cdot 17$ this would imply $5 \mid (x^2+1)$ and $17 \mid (x^2+1)$. Conversely if $5 \mid (x^2+1)$ and $17 \mid (x^2+1)$ then $85 \mid (x^2+1)$ by Theorem 1.7.6.

So solving the given equation is the same as solving the system

$$\begin{aligned} x^2 &\equiv -1 \pmod 5 \\ x^2 &\equiv -1 \pmod{17}. \end{aligned}$$

The equation $x^2 \equiv -1 \pmod 5$ clearly has solutions $x \equiv \pm 2 \pmod 5$ and $x^2 \equiv -1 \pmod{17}$ has solutions $x \equiv \pm 4 \pmod{17}$. There are four choices altogether, and each will reassemble into a solution mod 85:

$x \equiv 2 \pmod 5$, $x \equiv 4 \pmod{17} \overset{\text{CRT}}{\Longrightarrow} x \equiv 72 \pmod{85}$.

$x \equiv 2 \pmod 5$, $x \equiv -4 \pmod{17} \overset{\text{CRT}}{\Longrightarrow} x \equiv 47 \pmod{85}$.

$x \equiv -2 \pmod 5$, $x \equiv 4 \pmod{17} \overset{\text{CRT}}{\Longrightarrow} x \equiv 38 \pmod{85}$.

$x \equiv -2 \pmod 5$, $x \equiv -4 \pmod{17} \overset{\text{CRT}}{\Longrightarrow} x \equiv 13 \pmod{85}$.

So $x \equiv 13, 38, 47$ or $72 \pmod{85}$.

26 Exercise Check the steps labelled CRT in the above calculation.

27 Exercise Solve the system $x \equiv 2 \pmod 3$, $x \equiv 4 \pmod 5$, $x \equiv 6 \pmod 7$.

28 Exercise Prove that if $\gcd(a, 561) = 1$ then $a^{560} \equiv 1 \pmod{561}$. Hint: factor 561 and use the CRT.

2.9. The order of an element

2.9.1 Definition Let $(\mathbb{Z}/n\mathbb{Z})^\times$ be the set of invertible elements mod n.

So $(\mathbb{Z}/n\mathbb{Z})^\times$ is a set with $\varphi(n)$ elements.

2.9.2 Example

- ★ $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$.
- ★ If p is prime, $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\}$.

Let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Since there are only a finite number of elements in $(\mathbb{Z}/n\mathbb{Z})^\times$, we must eventually get $a^r \equiv a^s \pmod n$ for some $r > s$. Since a is invertible mod n we can multiply by a^{-1} s times and use theorem 2.6.10 to conclude that $a^{r-s} \equiv 1 \pmod n$. Thus for each a, $a^k \equiv 1 \pmod n$ for some positive integer k.

2.9.3 Definition The *order* of $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ is the least positive integer k such that $a^k \equiv 1 \pmod n$.

2.9.4 Example Calculate the order of 2 mod 5.

Solution: The powers of 2 mod 5 are

n	1	2	3	4
2^n	2	4	3	1

So the order of 2 is 4.

2.9.5 Example Calculate the order of 2 mod 11.

Solution: The powers of 2 mod 11:

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	5	10	9	7	3	6	1

So the order is 10.

2.9.6 Example Calculate the order of each invertible element mod 7.

Solution: Consider the table of powers mod 7:

x	x^2	x^3	x^4	x^5	x^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

Thus 1 has order 1, 6 has order 2, 2 and 4 have order 3, and 3 and 5 have order 6.

x	1	2	3	4	5	6
Order of x	1	3	6	3	6	2

2.9.7 Example 1 always has order 1, and every other element in $(\mathbb{Z}/n\mathbb{Z})^\times$ has order greater than 1.

Warning: If $a^m \equiv 1 \pmod{n}$ this does *not* imply that a has order m, because m may not be the *least* exponent with $a^m \equiv 1$. For example, $2^6 \equiv 1 \pmod{7}$, but the order of 2 is 3, not 6. In fact we have the following.

2.9.8 Theorem Let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ and let $m \in \mathbb{N}$. Then $a^m = 1$ iff m is a multiple of the order of a.

Proof Let the order of a be t.

$\Longrightarrow$ Suppose $a^m = 1$. Use the Division Algorithm to write $m = qt + r$ with $0 \le r < t$. Then

$$1 \equiv a^m = a^{qt+r} = (a^t)^q \cdot a^r \equiv 1^q \cdot a^r = a^r \pmod{n}.$$

Since $0 \le r < t$, the definition of order implies that $r = 0$. Thus t divides m.

$\Longleftarrow$ If $m = qt$ then $a^m = (a^t)^q \equiv 1^q = 1 \pmod{n}$. □

2.9.9 Corollary Let t be the order of $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $a^r \equiv a^s$ iff $r \equiv s \pmod{t}$.

Proof $a^r \equiv a^s$ iff $a^{r-s} \equiv 1$ iff $t \mid (r-s)$ by theorem 2.9.8. □

2.9.10 Corollary Let t be the order of $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $1, a, a^2, \ldots, a^{t-1}$ are all distinct mod n.

Proof Suppose $0 \le s < r < t$. If $a^r \equiv a^s$ then $t \mid (r-s)$ by the previous corollary. But $0 < r - s < t$ and there is no multiple of t in the interval $(0, t)$, contradiction. □

2.10. Primitive Roots

Let t be the order of $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. We know that $1, a, a^2, \ldots, a^{t-1}$ are all distinct mod n. Thus if t should happen to be $\varphi(n)$, *every* element of $(\mathbb{Z}/n\mathbb{Z})^\times$ will be a power of a.

2.10.1 Definition Let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. If the order of a is $\varphi(n)$ then a is called a *primitive root* mod n.

2.10.2 Example

- ★ By example 2.9.4 the order of 2 mod 5 is $4 = \varphi(5)$, so 2 is a primitive root mod 5. And indeed, the powers of 2 give all invertible elements mod 5.
- ★ By example 2.9.5 the order of 2 mod 11 is $10 = \varphi(10)$, so 2 is a primitive root mod 11. The powers of 2 give all invertible elements mod 11.
- ★ By example 2.9.6 the order of 2 mod 7 is $3 \neq \varphi(7) = 6$. Only 3 elements are powers of 2 mod 7, so 2 is not a primitive root mod 7. However the order of 3 mod 7 is 6, so 3 is a primitive root mod 7.

Primitive roots can be useful in solving equations mod n involving exponents. The idea is to write everything mod n in terms of powers of the primitive root, and then use Corollary 2.9.9.

2.10.3 Example Solve the equation $x^7 \equiv 5 \pmod{11}$.

Solution: 2 is a primitive root mod 11. Recall the table of Example 2.9.5:

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	5	10	9	7	3	6	1

Thus $5 \equiv 2^4$. Moreover, since every non-zero element of $\mathbb{Z}/11\mathbb{Z}$ is a power of 2 (and $x \equiv 0$ is clearly not a solution), we can write $x \equiv 2^y$ for some integer y. The equation becomes

$$2^{7y} \equiv 2^4 \pmod{11}.$$

By Corollary 2.9.9,

$$7y \equiv 4 \pmod{10}.$$

Warning: the new equation is taken modulo the order of 2*, which is 10, not 11.* Now $7^{-1} \equiv 3 \pmod{10}$, so multiplying by 3, $y \equiv 3 \cdot 4 \equiv 2 \pmod{10}$. Hence $x \equiv 2^2 \equiv 4 \pmod{11}$.

Check: $4^7 \equiv 5 \pmod{11}$. □

Unfortunately primitive roots do not always exist.

2.10.4 Example There is no primitive root mod 8.

Proof $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$. But $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$ so every element of $(\mathbb{Z}/8\mathbb{Z})^\times$ has order at most 2, and nothing has order $\varphi(8) = 4$.

The complete story is as follows:

2.10.5 Theorem There exists a primitive root mod n iff $n = 2, 4, p^k$ or $2p^k$ where p is an odd prime and $k \in \mathbb{N}$. In particular, there always exist primitive roots mod p.

Proof Omitted. □

2.11. Fermat's Little Theorem

We know that for each element a in $(\mathbb{Z}/n\mathbb{Z})^\times$ we can find an exponent m with $a^m \equiv 1 \pmod{n}$. But more is true: there is actually a single power that works for all a.

2.11.1 Theorem [Euler] Let $n \in \mathbb{N}$. Suppose $a \in \mathbb{Z}$ and $\gcd(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof Deferred until the algebra section. □

Note that this does *not* say that the order of every element is $\varphi(n)$. It only implies that the order of every element *divides* $\varphi(n)$. Indeed for many n primitive roots do not exist, so no element has order $\varphi(n)$.

2.11.2 Example Recall the table of powers mod 7:

x	x^2	x^3	x^4	x^5	x^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

We see that $a^6 \equiv 1 \pmod{n}$ for each a, as predicted by Euler's Theorem.

2.11.3 Corollary [Fermat's Little Theorem] Let p be prime. Suppose $a \in \mathbb{Z}$ is not divisible by p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof Take $n = p$ in Euler's Theorem. Then $\varphi(n) = p - 1$. □

2.11.4 Corollary Let p be prime. Then every integer a satisfies

$$a^p \equiv a \pmod{p}.$$

Proof If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$, so the result follows on multiplying through by a. If $p \mid a$ then $a \equiv 0 \pmod{p}$ and the result is obvious. □

2.11.5 Example Find $3^{100} \pmod{101}$. (Note: 101 is prime.)

Solution: By Fermat's Little Theorem $3^{100} \equiv 1 \pmod{101}$. Indeed $a^{100} \equiv 1 \pmod{101}$ for any $a \not\equiv 0 \pmod{101}$.

29 Exercise Check by repeated squaring that $a^{100} \equiv 1 \pmod{101}$ for $a = 2$, 3, 4 and 5.

2.11.6 Example Calculate $5^{1000000} \pmod{18}$.

Solution: $\varphi(18) = \varphi(2)\varphi(3^2) = 1 \cdot 3(3-1) = 6$, so $5^6 \equiv 1 \pmod{18}$, by Euler's Theorem. Now $1000000 = 6 \cdot 166666 + 4$, so

$$5^{1000000} \equiv (5^6)^{166666} \cdot 5^4 \equiv 1^{166666} \cdot 5^4 \equiv 25^2 \equiv 7^2 \equiv 13 \pmod{18}.$$

Unfinished Tasks:

(a) To prove Euler's Theorem, we need to show that the order of any element in $(\mathbb{Z}/n\mathbb{Z})^\times$ divides $\varphi(n)$, which is the number of elements in the set $(\mathbb{Z}/n\mathbb{Z})^\times$.

(b) We need to prove: if $\gcd(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$. That is,

$$|(\mathbb{Z}/mn\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times| \cdot |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

2.12. Applications: RSA

We discuss an *encryption scheme:* a way of sending messages so that no unauthorized person can read them. For the purpose of this discussion, a *message* will be an integer x in a specified range $0 < x < N$. This is not restrictive: any computer file ultimately consists of numbers. These may be split into blocks of numbers in the given range. In this way we may send text, images, audio, video etc (jpeg, mpeg, pdf etc).

RSA is a widely used encryption algorithm, developed by Rivest, Shamir and Adleman in 1977. Prior to RSA cryptosystems relied on a single secret value or "key". Knowledge of the key was required both to encrypt and to decrypt messages.

RSA was revolutionary, in that *one key is used to encrypt and a different key is used to decrypt.* The key used for encryption is made widely available, and is called the *public key* . Thus *anyone can encrypt a message.* The decryption key is called the *private key* and is kept secret. Once encrypted, a message cannot be read without knowing the private key.

In summary: anyone can send you a encrypted message. But only you can read it.

The algorithm is as follows:

2.12.1 Algorithm [RSA]

- Choose large primes p and q (each with at least 100 decimal digits).
- Calculate $N = pq$ and $\varphi(N) = (p-1)(q-1)$. Choose a random integer e with $\gcd(e, \varphi(N)) = 1$.
- Using Euclid's algorithm, calculate $d = e^{-1} \pmod{\varphi(N)}$.
- Publish the *public key* (N, e). Retain the *private key* d.
- A message will be an integer x with $0 < x < N$.
- Encryption: If someone wants to send you a message x they encrypt it by instead sending $x^e \pmod{N}$.
- Decryption: To decrypt a received message y, calculate $y^d \pmod{N}$.

2.12.2 Theorem RSA works.

Proof Since $ed \equiv 1 \pmod{\varphi(N)}$, we know $ed = 1 + t\varphi(N)$ for some integer t. If we receive $y \equiv x^e$, we calculate

$$y^d \equiv (x^e)^d \equiv x^{ed} \equiv x \cdot (x^{\varphi(N)})^t \pmod{N}.$$

Assume that $\gcd(x, N) = 1$. (See exercises for the case $\gcd(x, N) > 1$.) By Euler's theorem $x^{\varphi(N)} \equiv 1 \pmod{N}$, so $y^d \equiv x \pmod{N}$ and we recover the original message. □

30 Exercise What happens if $\gcd(x, N) > 1$ in RSA? Then we cannot use Euler's theorem. Check the following argument.

Instead of using Euler's theorem, work mod p:

$$\begin{aligned} y^d &\equiv x \cdot (x^{\varphi(N)})^t = x \cdot x^{(p-1)(q-1)t} \equiv x \cdot \left[x^{(p-1)}\right]^{(q-1)t} \\ &\equiv \begin{cases} 0 \pmod{p}, & \text{if } p \mid x \\ x \cdot 1 \pmod{p}, & \text{if } p \nmid x \end{cases} \end{aligned}$$

where we used Fermat's Little Theorem at the last step. So $y^d \equiv x \pmod{p}$ in all cases, so $p \mid (y^d - x)$. Similarly, $q \mid (y^d - x)$. By Theorem 1.7.6, $N = pq \mid (y^d - x)$, so $x \equiv y \pmod{N}$ for all possible messages x.

31 Exercise If $N = pq$ with p, q each about 10^{100}, estimate $\phi(N)/N$. This is the probability that a random x mod N will have $\gcd(x, N) > 1$. Comment on the likelihood of this case arising.

32 Exercise If $\gcd(x, N) > 1$ explain why we can immediately break RSA. (See the next section.) So the validity of the algorithm is a moot point in this case.

2.12.3 Example We give an example of RSA with small numbers. Choose $p = 5$, $q = 11$. Then $N = pq = 55$, $\varphi(N) = 4 \cdot 10 = 40$. Let us choose $e = 3$. Note that $\gcd(e, \varphi(N)) = \gcd(3, 40) = 1$. We need to find $d \equiv e^{-1} \pmod{40}$. By Euclid's algorithm, $d = 27$.

The public key is $(N, e) = (55, 3)$. The private key is $d = 27$. A message will be an integer x with $0 < x < 55$.

Example: To send message $x = 18$, we calculate

$$x^3 \equiv 2 \pmod{55}.$$

The encrypted message is 2. To decrypt, use the private key $d = 27$ and calculate

$$2^{27} \equiv 18 \pmod{55}.$$

33 Exercise Let $(N, e) = (323, 11)$. Suppose you intercept an encrypted message 316. Break the cipher and decrypt the message. Hint: you will have to factor N.

2.13. The Security of RSA

The public key (N, e) is available to everyone. The cipher is broken if d is found. Since $de \equiv 1 \pmod{\varphi(N)}$, RSA is immediately broken if $\varphi(N)$ can be calculated from N, since then we can quickly find d using Euclid's algorithm.

2.13.1 Theorem Finding $\varphi(N)$ is equivalent to factoring N.

Proof

$\Longrightarrow$ Suppose $\varphi(N)$ is somehow found. Then

$$\varphi(N) = (p-1)(q-1) = pq - (p+q) + 1 = N - (p+q) + 1$$

so

$$p + q = N - \varphi(N) + 1.$$

Hence $p + q$ can be found. But

$$(p - q)^2 = (p + q)^2 - 4pq = (p + q)^2 - 4N$$

so

$$p - q = \sqrt{(p + q)^2 - 4N}.$$

can also be found. Once we know $p - q$ and $p + q$ we recover p and q by adding and subtracting these quantities.

$\Longleftarrow$ If we know the factorization of N is $N = pq$ then $\varphi(N) = (p - 1)(q - 1)$ is easily found. $\square$

Thus:

The security of RSA entirely depends on the difficulty of factoring a large integer into its prime factors.

Of course, the factors can always be found eventually, but even with the best algorithms known, if N has 400 digits, this would take trillions of times the age of the universe ...

Nonetheless, RSA is not *proved* to be secure. No one has proved[2] that no rapid algorithm for factoring exists—this is related to the so called $P = NP$ problem in computer science. Furthermore, it is known that factoring can be done rapidly if one can build a so called quantum computer. Whether or not this will be possible any time soon (or ever) is a matter of conjecture ...

[2]Also, we prove that finding $\varphi(N)$ is as hard as factoring N. But possibly there is some way to break RSA without finding $\varphi(N)$?

Part 2

Abstract algebra