# II NUMBER THEORY

We use the need to send secret messages as the motivation to study questions in number theory. The main tool for this purpose is modular integer arithmetic.

# 4 Modular Arithmetic

We begin the chapter on number theory by introducing modular integer arithmetic. One of its uses is in the encryption of secret messages. In this section, all numbers are integers.

**Private key cryptography.** The problem of sending secret messages is perhaps as old as humanity or older. We have a *sender* who attempts to encrypt a message in such a way that the intended *receiver* is able to decipher it but any possible *adversary* is not. Following the traditional protocol, the sender and receiver agree on a secret code ahead of time, and they use it to both encrypt and decipher the message. The weakness of the method is the secret code, which may be stolen or cracked.

As an example, consider *Ceasar's cipher*, which consists of shifting the alphabet by some fixed number of positions, e.g.,

$$\begin{array}{ccccccccc} A & B & C & \dots & V & W & X & Y & Z \\ \downarrow & \downarrow & \downarrow & \dots & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ E & F & G & \dots & Z & A & B & C & D. \end{array}$$

If we encode the letters as integers, this is the same as adding a fixed integer but then subtracting 26, the number of letters, if the sum exceeds this number. We consider this kind of integer arithmetic more generally.

**Public key cryptography.** Today, we use more powerful encryption methods that give a more flexible way to transmit secret information. We call this *public key cryptography* which roughly works as follows. As before, we have a sender, called Alice, and a receiver, called Bob. Both Alice and Bob have a *public key*, $KP_A$ and $KP_B$, which they publish for everyone to see, and a *secret key*, $KS_A$ and $KS_B$, which is only known to themselves. They do not exchange the secret key even among each other. The keys are used to change messages so we can think of them as functions. The function that corresponds to the public and the secret keys are inverses of each other, that is,

$$\begin{aligned} S_A(P_A(x)) &= P_A(S_A(x)) = x; \\ S_B(P_B(x)) &= P_B(S_B(x)) = x. \end{aligned}$$

The crucial point is that $P_A$ is easy to compute for everybody and $S_A$ is easy to compute for Alice but difficult for everybody else, including Bob. Symmetrically, $P_B$ is easy for everybody but $S_B$ is easy only for Bob. Perhaps this sound contradictory since everybody knows $P_A$ and $S_A$ is just its inverse, but it turns out that there are pairs of functions that satisfy this requirement. Now, if Alice wants to send a message to Bob, she proceeds as follows:

1. Alice gets Bob's public key, $P_B$.
2. Alice applies it to encrypt her message, $y = P_B(x)$.
3. Alice sends $y$ to Bob, publically.
4. Bob applies $S_B(y) = S_B(P_B(x)) = x$.

We note that Alice does not need to know Bob's secret key to encrypt her message and she does not need secret channels to transmit her encrypted message.

**Arithmetic modulo $n$.** We begin by defining what it means to take one integer, $m$, modulo another integer, $n$.

DEFINITION. Letting $n \leq 1$, $m \bmod n$ is the smallest integer $r \geq 0$ such that $m = nq + r$ for some integer $q$.

Given $m$ and $n \geq 1$, it is not difficult to see that $q$ and $r$ exist. Indeed, $n$ partitions the integers into intervals of length $n$:

$$\dots, -n, \dots, 0, \dots, n, \dots, 2n, \dots$$

The number $m$ lies in exactly one of these intervals. More precisely, there is an integer $q$ such that $qn \leq m < ((q + 1)n$. The integer $r$ is the amount by which $m$ exceeds $qn$, that is, $r = m - qn$. We see that $q$ and $r$ are unique, which is known as

EUCLID'S DIVISION THEOREM. Letting $n \geq 1$, for every $m$ there are unique integers $q$ and $0 \leq r < n$ such that $m = nq + r$.

**Computations.** It is useful to know that modulos can be taken anywhere in the calculation if it involves only addition and multiplication. We state this more formally.

LEMMA 1. Letting $n \geq 1$, $i \bmod n = (i + kn) \bmod n$.

This should be obvious because adding $k$ times $n$ moves the integer $i$ to the right by $k$ intervals but maintains its relative position within the interval.

LEMMA 2. Letting $n \geq 1$, we have

$$\begin{aligned} (i + j) \bmod n &= (i \bmod n) + (j \bmod n) \bmod n; \\ (i \cdot j) \bmod n &= (i \bmod n) \cdot (j \bmod n) \bmod n. \end{aligned}$$

PROOF. By Euclid's Division Theorem, there are unique integers $q_i, q_j$ and $0 \le r_i, r_j < n$ such that

$$\begin{aligned} i &= q_i n + r_i; \\ j &= q_j n + r_j. \end{aligned}$$

Plugging this into the left hand side of the first equation, we get

$$\begin{aligned} (i+j) \bmod n &= (q_i + q_j)n + (r_i + r_j) \bmod n \\ &= (r_i + r_j) \bmod n \\ &= (i \bmod n) + (j \bmod n) \bmod n. \end{aligned}$$

Similarly, it is easy to show that $(ij) \bmod n = (r_i r_j) \bmod n$, which implies the second equation. □

**Algebraic structures.** Before we continue, we introduce some notation. Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and write $+_n$ for addition modulo $n$. More formally, we have an operation that maps two numbers, $i \in \mathbb{Z}_n$ and $j \in \mathbb{Z}_n$, to their sum, $i +_n j = (i+j) \bmod n$. This operation satisfies the following four properties:

- it is *associative*, that is, $(i +_n j) +_n k = i +_n (j +_n k)$ for all $i, j, k \in \mathbb{Z}_n$;
- $0 \in \mathbb{Z}_n$ is the *neutral element*, that is, $0 +_n i = i$ for all $i \in \mathbb{Z}_n$;
- every $i \in \mathbb{Z}_n$ has an *inverse element* $i'$, that is, $i +_n i' = 0$;
- it is *commutative*, that is, $i +_n j = j +_n i$ for all $i, j \in \mathbb{Z}_n$.

The first three are the defining property of a *group*, and if the fourth property is also satisfied we have a *commutative* or *Abelian group*. Thus, $(\mathbb{Z}_n, +_n)$ is an Abelian group. We have another operation mapping $i$ and $j$ to their product, $i \cdot_n j = (ij) \bmod n$. This operation has a similar list of properties:

- it is *associative*, that is, $(i \cdot_n j) \cdot_n k = i \cdot_n (j \cdot_n k)$ for all $i, j, k \in \mathbb{Z}_n$;
- $1 \in \mathbb{Z}_n$ is the *neutral element*, that is, $1 \cdot_n i = i$ for all $i \in \mathbb{Z}_n$;
- it is *commutative*, that is, $i \cdot_n j = j \cdot_n i$ for all $i, j \in \mathbb{Z}_n$.

Under some circumstances, we also have inverse elements but not in general. Hence, $(\mathbb{Z}_n, \cdot_n)$ is generally not a group. Considering the interaction of the two operations, we note that

- multiplication *distributes* over addition, that is, $i \cdot_n (j +_n k) = (i \cdot_n j) +_n (i \cdot_n k)$ for all $i, j, k \in \mathbb{Z}_n$.

These are the eight defining properties of a *commutative ring*. Had we also a multiplicative inverse for every non-zero element then the structure would be called a *field*. Hence, $(\mathbb{Z}_n, +_n, \cdot_n)$ is a commutative ring. We will see in the next section that it is a field if $n$ is a prime number.

**Addition and multiplication modulo $n$.** We may be tempted to use modular arithmetic for the purpose of transmitting secret messages. As a first step, the message is interpreted as an integer, possibly a very long integer. For example, we may write each letter in ASCII and read the bit pattern as a number. Then we concatenate the numbers. Now suppose Alice and Bob agree on two integers, $n \ge 1$ and $a$, and they exchange messages using

$$\begin{aligned} P(x) &= x +_n a; \\ S(y) &= y +_n (-a) = y -_n a. \end{aligned}$$

This works fine but not as a public key cryptography system. Knowing that $P$ is the same as adding $a$ modulo $n$, it is easy to determine its inverse, $S$. Alternatively, let us use multiplication instead of addition,

$$\begin{aligned} P(x) &= x \cdot_n a; \\ S(y) &= y \cdot_n (-a) = y :_n a. \end{aligned}$$

The trouble now is that division modulo $n$ is not as straightforward an operation as for integers. Indeed, if $n = 12$ and $a = 4$, we have $0 \cdot 4 = 3 \cdot 4 = 6 \cdot 4 = 9 \cdot 4 = 0 \bmod n$. Since multiplication with $4$ is not injective, the inverse operation is not well defined. Indeed, $0 :_n 4$ could be 0, 3, 6, or 9.

**Summary.** We learned about private and public key cryptography, ways to to send a secret message from a sender to a receiver. We also made first steps into number theory, introducing modulo arithmetic and Euclid's Division Theorem. We have seem that addition and multiplication modulo $n$ are both commutative and associative, and that multiplication distributes over addition, same as in ordinary integer arithmetic.

# 5 Inverses

In this section, we study under which conditions there is a multiplicative inverse in modular arithmetic. Specifically, we consider the following four statements.

I. The integer $a$ has a multiplicative inverse in $\mathbb{Z}_n$.

II. The linear equation $a \cdot_n x = b$ has a solution in $\mathbb{Z}_n$.

III. The linear equation $ax + ny = 1$ has a solution in the integers.

IV. The integers $a$ and $n$ are relative prime.

We will see that all four statements are equivalent, and we will prove all necessary implications to establish this, except for one, which we will prove in the next section.

**Examples.** Before starting the proofs, we compute multiplicative inverses for a few values of $n$ and $a$; see Table 1. Except for $a = 0$, all values of $a$ have multiplicative inverses if $n = 2, 3, 5, 7$ but not if $n = 4, 6, 8, 9$. In the latter case, we have multiplicative inverses for some values of $a$ but not for all. We will later find out that the characterizing condition for the existence of the multiplicative inverse is that $n$ and $a$ have no non-trivial common divisor.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $n=2$ | $a$ | 0 | 1 | | | | | | |
| | $a'$ | | 1 | | | | | | |
| $n=3$ | $a$ | 0 | 1 | 2 | | | | | |
| | $a'$ | | 1 | 2 | | | | | |
| $n=4$ | $a$ | 0 | 1 | 2 | 3 | | | | |
| | $a'$ | | 1 | | 3 | | | | |
| $n=5$ | $a$ | 0 | 1 | 2 | 3 | 4 | | | |
| | $a'$ | | 1 | 2 | 3 | 4 | | | |
| $n=6$ | $a$ | 0 | 1 | 2 | 3 | 4 | 5 | | |
| | $a'$ | | 1 | | | | 5 | | |
| $n=7$ | $a$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | |
| | $a'$ | | 1 | 4 | 5 | 2 | 3 | 6 | |
| $n=8$ | $a$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | $a'$ | | 1 | | 3 | | 5 | | 7 |
| $n=9$ | $a$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | $a'$ | | 1 | 5 | | 7 | 2 | | 4 | 8 |

Table 1: Values of $n$ for which $a$ has a multiplicative inverse $a'$. Black entries indicate the inverse does not exist.

**Linear equations modulo $n$.** Here we prove I $\iff$ II. The *multiplicative inverse* of an integer $a \in \mathbb{Z}_n$ is another integer $a' \in \mathbb{Z}_n$ such that $a' \cdot_n a = a \cdot_n a' = 1$. We note that the multiplicative inverse is unique, if it exists. Indeed, if $a'' \cdot_n a = 1$ then we can multiply with $a'$ from the right and get $a' \cdot_n (a \cdot_n a') = a'' \cdot_n (a \cdot_n a')$ and therefore $a' = a''$. If $a$ has a multiplicative inverse, we can use it to solve a linear equation. Multiplying with the inverse from the left and using associativity, we get

$$\begin{aligned} a \cdot_n x &= b; \\ (a' \cdot_n a) \cdot_n x &= a' \cdot_n b; \\ x &= a' \cdot_n b. \end{aligned}$$

Since the multiplicative inverse is unique, so is the solution $x = a' \cdot_n b$ to the linear equation. We thus proved a little bit more than I $\implies$ II, namely also the uniqueness of the solution.

A. If $a$ has a multiplicative inverse $a'$ in $\mathbb{Z}_n$ then for every $b \in \mathbb{Z}_n$, the equation $a \cdot_n x = b$ has the unique solution $x = a' \cdot_n b$.

Every implication has an equivalent contrapositive form. For a statement I $\implies$ II this form is $\neg$II $\implies \neg$I. We state the contrapositive form in this particular instance.

A'. If $a \cdot_n x = b$ has no solution in $\mathbb{Z}_n$ then $a$ does not have a multiplicative inverse.

To prove A' we just need to assume that it is false, that is, that $\neg$II and I both hold. But if we have I then we also have II. Now we have $\neg$II as well as II. But this is a contradiction with they cannot both be true. What we have seen here is a very simple version of a proof by contradiction. More complicated versions will follow later.

By setting $b = 1$, we get $x = a'$ as a solution to $a \cdot_n x = 1$. In other words, $a' \cdot_n a = a \cdot_n a' = 1$. Hence, II $\implies$ I. This particuar implication is called the converse of I $\implies$ II, which should not be confused with the contrapositive. The converse is a new, different statement, while the contrapositive is logically eqivalent to the original implication, no matter what the specifics of the implication are.

**Linear equations in two variables.** Here we prove II $\iff$ III. Recall that $a \cdot_n x = 1$ is equivalent to $ax \bmod n = 1$. Writing $ax = qn + r$ with $0 \le r < n$, we see that $ax \bmod n = 1$ is equivalent to the existence of an integer $q$ such that $ax = qn + 1$. Writing $y = -q$ we get

$$ax + ny = 1.$$

All steps in the above derivation are reversible. Hence, we proved that II is equivalent to III. We state the specific result.

B. The equation $a \cdot_n x = b$ has a solution in $\mathbb{Z}_n$ iff there exist integers $x$ and $y$ such that $ax + ny = 1$.

Implications are transitive, that is, if I implies II and II implies III then I implies III. We can do the same chain of implications in the other direction as well. Hence, if I $\iff$ II and II $\iff$ III, as we have established above, we also have I $\iff$ III. We again state this specific result for clarity.

C. The integer $a$ has a multiplicative inverse in $\mathbb{Z}_n$ iff there exist integers $x$ and $y$ such that $ax + ny = 1$.

**Greatest common divisors.** Here we prove III $\implies$ IV. We will prove IV $\implies$ III later. We say an integer $i$ *factors* another integer $j$ if $j/i$ is an integer. Furthermore, $j$ is a *prime number* if its only factors are $\pm j$ and $\pm 1$. The *greatest common divisor* of two integers $j$ and $k$, denoted as $\gcd(j, k)$, is the largest integer $d$ that is a factor of both. We say $j$ and $k$ and *relative prime* if $\gcd(j, k) = 1$.

D. Given integers $a$ and $n$, if there exist integers $x$ and $y$ such that $ax + ny = 1$ then $\gcd(a, n) = 1$.

PROOF. Suppose $\gcd(a, n) = k$. Then we can write $a = ik$ and $n = jk$. Substituting these into the linear equation gives

$$\begin{aligned} 1 &= ax + ny \\ &= k(ix + jy). \end{aligned}$$

But then $k$ is a factor of 1 and therefore $k = \pm 1$. This implies that the only common factors of $a$ and $n$ are $\pm 1$ and therefore $\gcd(a, n) = 1$. □

**Summary.** We have proved relationships between the statements I, II, III, IV; see Figure 5. We will see later that

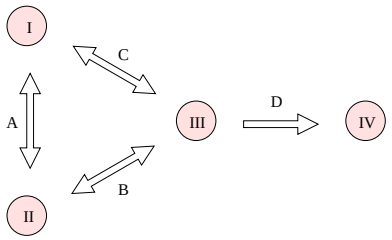


Figure 5: Equivalences between statements.

the implication proved by D can also be reversed. Thus computing the greatest common divisor gives a test for the existence of a multiplicative inverse.

# 6 Euclid's Algorithm

In this section, we present Euclid's algorithm for the greatest common divisor of two integers. An extended version of this algorithm will furnish the one implication that is missing in Figure 5.

**Reduction.** An important insight is Euclid's Division Theorem stated in Section 4. We use it to prove a relationship between the greatest common divisors of numbers $j$ and $k$ when we replace $k$ by its remainder modulo $j$.

LEMMA. Let $j, k, q, r > 0$ with $k = jq + r$. Then $\gcd(j, k) = \gcd(r, j)$.

PROOF. We begin by showing that every common factor of $j$ and $k$ is also a factor of $r$. Letting $d = \gcd(j, k)$ and writing $j = Jd$ and $k = Kd$, we get

$$r \;=\; k - jq \;=\; (K - Jq)d.$$

We see that $r$ can be written as a multiple of $d$, so $d$ is indeed a factor of $r$. Next, we show that every common factor of $r$ and $j$ is also a factor of $k$. Letting $d = \gcd(r, j)$ and writing $r = Rd$ and $j = Jd$, we get

$$k \;=\; jq + r \;=\; (Jq + R)d.$$

Hence, $d$ is indeed a factor of $k$. But this implies that $d$ is a common factor of $j$ and $k$ iff it is a common factor of $r$ and $j$. □

**Euclid's gcd algorithm.** We use the Lemma to compute the greatest common divisor of positive integers $j$ and $k$. The algorithm is recursive and reduces the integers until the remainder vanishes. It is convenient to assume that both integers, $j$ and $k$, are positive and that $j \leq k$.

```
integer GCD(j, k)
  q = k div j; r = k − jq;
  if r = 0 then return j
           else return GCD(r, j)
  endif.
```

If we call the algorithm for $j > k$ then the first recursive call is for $k$ and $j$, that is, it reverses the order of the two integers and keeps them ordered as assumed from then on. Note also that $r < j$. In words, the first parameter, $j$, shrinks in each iterations. There are only a finite number of non-negative integers smaller than $j$ which implies that after a finite number of iterations the algorithm halts with $r = 0$. In other words, the algorithm terminates after a finite number of steps, which is something one should always check, in particular for recursive algorithms.

**Last implication.** We modify the algorithm so it also returns the integers $x$ and $y$ for which $\gcd(j, k) = jx+ky$. This provides the missing implication in Figure 5.

D'. If $\gcd(a, n) = 1$ then the linear equation $ax+ny = 1$ has a solution.

This finally verifies that the gcd is a test for the existence of a multiplicative inverse in modular arithmetic. More specifically, $x \bmod n$ *is* the multiplicative inverse of $a$ in $\mathbb{Z}_n$. Do you see why? We can thus update the relationship between the statements I, II, III, IV listed at the beginning of Section 5; see Figure 6.

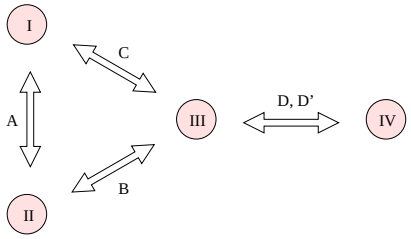


Figure 6: Equivalences between the statements listed at the beginning of Section 5.

**Extended gcd algorithm.** If $r = 0$ then the above algorithm returns $j$ as the gcd. In the extended algorithm, we also return $x = 1$ and $y = 0$. Now suppose $r > 0$. In this case, we recurse and get

$$\begin{aligned} \gcd(r, j) &= rx' + jy' \\ &= (k - jq)x' + jy' \\ &= j(y' - qx') + kx'. \end{aligned}$$

We thus return $g = \gcd(r, j)$ as well as $x = y' - qx'$ and $y = x'$. As before, we assume $0 < j \leq k$ when we call the algorithm.

```
integer³ xGCD(j, k)
  q = k div j; r = k − jq;
  if r = 0 then return (j, 1, 0)
           else (g, x', y') = xGCD(r, j);
                return (g, y' − qx', x')
  endif.
```

To illustrate the algorithm, we run it for $j = 14$ and $k = 24$. The values of $j, k, q, r, g = \gcd(j,k), x, y$ at the various levels of recursion are given in Table 2.

| $j$ | $k$ | $q$ | $r$ | $g$ | $x$ | $y$ |
|---|---|---|---|---|---|---|
| 14 | 24 | 1 | 10 | 2 | -5 | 3 |
| 10 | 14 | 1 | 4 | 2 | 3 | -2 |
| 4 | 10 | 2 | 2 | 2 | -2 | 1 |
| 2 | 4 | 2 | 0 | 2 | 1 | 0 |

Table 2: Running the extended gcd algorithm on $j = 14$ and $k = 24$.

**Computing inverses.** We have established that the integer $a$ has a multiplicative inverse in $\mathbb{Z}_n$ iff $\gcd(a,n) = 1$. Assuming $n = p$ is a prime number, this is the case whenever $a < p$ is positive.

COROLLARY. If $p$ is prime then every non-zero $a \in \mathbb{Z}_p$ has a multiplicative inverse.

It is straightforward to compute the multiplicative inverse using the extended gcd algorithm. As before, we assume $p$ is a prime number and $0 < a < p$.

```
integer INVERSE(a, p)
  (g, x, y) = xGCD(a, p);
  assert g = 1; return x mod p.
```

The assert statement makes sure that $a$ and $p$ are indeed relative prime, for else the multiplicative inverse would not exist. We have seen that $x$ can be negative so it is necessary to take $x$ modulo $p$ before we report it as the multiplicative inverse.

**Multiple moduli.** Sometimes, we deal with large integers, larger then the ones that fit into a single computer word (usually 32 or 64 bits). In this situation, we have to find a representation that spreads the integer over several words. For example, we may represent an integer $x$ by its remainders modulo 3 and modulo 5, as shown in Table 3. We see that the first 15 non-negative integers correspond to different pairs of remainders. The generalization of this insight to relative prime numbers $m$ and $n$ is known as the

| $x$ | 0 | 1 | 2 | 3 | 4 | ... | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|
| $x \bmod 3$ | 0 | 1 | 2 | 0 | 1 | ... | 1 | 2 | 0 |
| $x \bmod 5$ | 0 | 1 | 2 | 3 | 4 | ... | 3 | 4 | 0 |

Table 3: Mapping the integers from 0 to 15 to pairs of remainders after dividing with 3 and with 5.

CHINESE REMAINDER THEOREM. Let $m, n > 0$ be relative prime. Then for every $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$, the system of two linear equations

$$\begin{aligned} x \bmod m &= a; \\ x \bmod n &= b \end{aligned}$$

has a unique solution in $\mathbb{Z}_{mn}$.

There is a further generalization to more then two moduli that are pairwise relative prime. The proof of this theorem works as suggested by the example, namely by showing that $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ defined by

$$f(x) = (x \bmod m, x \bmod n)$$

is injective. Since both $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ have size $mn$, this implies that $f$ is a bijection. Hence, $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ has a unique preimage, the solution of the two equations.

To use this result, we would take two large integers, $x$ and $y$, and represent them as pairs, $(x \bmod m, x \bmod n)$ and $(x \bmod m, x \bmod n)$. Arithmetic operations can then be done on the remainders. For example, $x$ times $y$ would be represented by the pair

$$\begin{aligned} xy \bmod m &= [(x \bmod m)(y \bmod m)] \bmod m; \\ xy \bmod n &= [(x \bmod n)(y \bmod n)] \bmod n. \end{aligned}$$

We would choose $m$ and $n$ small enough so that multiplying two remainders can be done using conventional, single-word integer multiplication.

**Summary.** We discussed Euclid's algorithm for computing the greatest common divisor of two integers, and its extended version which provides the missing implication in Figure 5. We have also learned the Chinese Remainder Theorem which can be used to decompose large integers into digestible junks.

# 7 RSA Cryptosystem

Addition and multiplication modulo $n$ do not offer the computational difficulties needed to build a viable cryptographic system. We will see that exponentiation modulo $n$ does.

**Operations as functions.** Recall that $+_n$ and $\cdot_n$ each read two integers and return a third integer. If we fix one of the two input integers, we get two functions. Specifically, fixing $a \in \mathbb{Z}_n$, we have functions $A : \mathbb{Z}_n \to \mathbb{Z}_n$ and $M : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by

$$\begin{aligned} A(x) &= x +_n a; \\ M(x) &= x \cdot_n a; \end{aligned}$$

see Table 4. Clearly, $A$ is injective for every choice of

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $A(x)$ | 2 | 3 | 4 | 5 | 0 | 1 |
| $M(x)$ | 0 | 2 | 4 | 0 | 2 | 4 |

Table 4: The function $A$ defined by adding $a = 2$ modulo $n = 6$ is injective. In contrast, the function $M$ defined by multiplying with $a = 2$ is not injective.

$n > 0$ and $a \in \mathbb{Z}_n$. On the other hand, $M$ is injective iff $\gcd(a, n) = 1$. In particular, $M$ is injective for every non-zero $a \in \mathbb{Z}_n$ if $n$ is prime.

**Exponentiation.** Yet another function we may consider is taking $a$ to the $x$-th power. Let $E : \mathbb{Z}_n \to \mathbb{Z}_n$ be defined by

$$\begin{aligned} E(x) &= a^x \bmod n \\ &= a \cdot_n a \cdot_n \ldots \cdot_n a, \end{aligned}$$

where we multiply $x$ copies of $a$ together. We see in Table 5 that for some values of $a$ and $n$, the restriction of $E$ to the non-zero integers is injective and for others it is not. Perhaps surprisingly, the last column of Table 5 consists of 1s only.

FERMAT'S LITTLE THEOREM. Let $p$ be prime. Then $a^{p-1} \bmod p = 1$ for every non-zero $a \in \mathbb{Z}_p$.

PROOF. Since $p$ is prime, multiplication with $a$ gives an injective function for every non-zero $a \in \mathbb{Z}_p$. In other words, multiplying with $a$ permutes the non-zero integers

| $a^x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 2 | 4 | 1 | 2 | 4 | 1 |
| 3 | 1 | 3 | 2 | 6 | 4 | 5 | 1 |
| 4 | 1 | 4 | 2 | 1 | 4 | 2 | 1 |
| 5 | 1 | 5 | 4 | 6 | 2 | 3 | 1 |
| 6 | 1 | 6 | 1 | 6 | 1 | 6 | 1 |

Table 5: Exponentiation modulo $n = 7$. We write $x$ from left to right and $a$ from top to bottom.

in $\mathbb{Z}_p$. Hence,

$$\begin{aligned} X &= 1 \cdot_p 2 \cdot_p \ldots \cdot_p (p-1) \\ &= (1 \cdot_p a) \cdot_p (2 \cdot_p a) \cdot_p \ldots \cdot_p ((p-1) \cdot_p a) \\ &= X \cdot_p (a^{p-1} \bmod p). \end{aligned}$$

Multiplying with the inverse of $X$ gives $a_{p-1} \bmod p = 1$. □

**One-way functions.** The RSA cryptosystem is based on the existence of *one-way functions* $f : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by the following three properties:

- $f$ is easy to compute;
- its inverse, $f^{-1} : \mathbb{Z}_n \to \mathbb{Z}_n$, exists;
- without extra information, $f^{-1}$ is hard to compute.

The notions of 'easy' and 'hard' computation have to be made precise, but this is beyond the scope of this course. Roughly, it means that given $x$, computing $y = f(x)$ takes on the order of a few seconds while computing $f^{-1}(y)$ takes on the order of years. RSA uses the following recipe to construct one-way functions:

1. choose large primes $p$ and $q$, and let $n = pq$;
2. choose $e \neq 1$ relative prime to $(p-1)(q-1)$ and let $d$ be its multiplicative inverse modulo $(p-1)(q-1)$;
3. the one-way function is defined by $f(x) = x^e \bmod n$ and its inverse is defined by $g(y) = y^d \bmod n$.

According to the RSA protocol, Bob publishes $e$ and $n$ and keeps $d$ private. To exchange a secret message, $x \in \mathbb{Z}_n$,

4. Alice computes $y = f(x)$ and publishes $y$;
5. Bob reads $y$ and computes $z = g(y)$.

To show that RSA is secure, we would need to prove that without knowing $p, q, d$, it is hard to compute $g$. We

leave this to future generations of computer scientists. Indeed, nobody today can prove that computing $p$ and $q$ from $n = pq$ is hard, but then nobody knows how to factor large integers efficiently either.

**Correctness.** To show that RSA works, we need to prove that $z = x$. In other words, $g(y) = f^{-1}(y)$ for every $y \in \mathbb{Z}_n$. Recall that $y$ is computed as $f(x) = x^e \bmod n$. We need $y^d \bmod n = x$ but we first prove a weaker result.

LEMMA. $y^d \bmod p = x \bmod p$ for every $x \in \mathbb{Z}_n$.

PROOF. Since $d$ is the multiplicative inverse of $e$ modulo $(p-1)(q-1)$, we can write $ed = (p-1)(q-1)k + 1$. Hence,

$$\begin{aligned} y^d \bmod p &= x^{ed} \bmod p \\ &= x^{k(p-1)(q-1)+1} \bmod p. \end{aligned}$$

Suppose first that $x^{k(q-1)} \bmod p \neq 0$. Then Fermat's Little Theorem implies $x^{k(p-1)(q-1)} \bmod p = 1$. But this implies $y^d \bmod p = x \bmod p$, as claimed. Suppose second that $x^{k(q-1)} \bmod p = 0$. Since $p$ is prime, every power of a non-zero integer is non-zero. Hence, $x \bmod p = 0$. But this implies $y^d \bmod p = 0$ and thus $y^d \bmod p = x \bmod p$, as before. □

By symmetry, we also have $y^d \bmod q = x \bmod q$. Hence,

$$\begin{aligned} (y^d - x) \bmod p &= 0; \\ (y^d - x) \bmod q &= 0. \end{aligned}$$

By the Chinese Remainder Theorem, this system of two linear equations has a unique solution in $\mathbb{Z}_n$, where $n = pq$. Since $y^d - x = 0$ is a solution, there can be no other. Hence,

$$(y^d - x) \bmod n = 0.$$

The left hand side can be written as $((y^d \bmod n) - x) \bmod n$. This finally implies $y^d \bmod n = x$, as desired.

**Summary.** We talked about exponentiation modulo $n$ and proved Fermat's Little Theorem. We then described how RSA uses exponentiation to construct one-way functions, and we proved it correct. A proof that RSA is secure would be nice but is beyond what is currently known.

# Second Homework Assignment

Write the solution to each problem on a single page. The deadline for handing in solutions is February 6.

**Question 1.** ($20 = 10 + 10$ points). (Problem 2.1-12 in our textbook). We recall that a prime number, $p$, that divides a product of integers divides one of the two factors.

(a) Let $1 \leq a \leq p-1$. Use the above recollection to show that as $b$ runs through the integers from 0 to $p-1$, the products $a \cdot_p b$ are all different.

(b) Explain why every positive integer less than $p$ has a unique multiplicative inverse in $\mathbb{Z}_p$.

**Question 2.** (20 points). (Problem 2.2-19 in our textbook). The *least common multiple* of two positive integers $i$ and $j$, denoted as $\mathrm{lcm}(i, j)$, is the smallest positive integer $m$ such that $m/i$ and $m/j$ are both integer. Give a formula for $\mathrm{lcm}(i, j)$ that involves $\gcd(i, j)$.

**Question 3.** ($20 = 10 + 10$ points). (Problem 2.2-17 in our textbook). Recall the Fibonacci numbers defined by $F_0 = 0$, $F_1 = 1$, and $F_i = F_{i-1} + F_{i-2}$ for all $i \geq 2$.

(a) Run the extended gcd algorithm for $j = F_{10}$ and $k = F_{11}$, showing the values of all parameters at all levels of the recursion.

(b) Running the extended gcd algorithm for $j = F_i$ and $k = F_{i+1}$, how many recursive calls does it take to get the result?

**Question 4.** (20 points). Let $n \geq 1$ be a nonprime and $x \in \mathbb{Z}_n$ such that $\gcd(x, n) \neq 1$. Prove that $x^{n-1} \bmod n \neq 1$.