Cryptography 101: Elementary Number Theory

1 The integers

The set of integers $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ is denoted by the symbol $\mathbb{Z}$.

Definition 1 Let a, b be integers. Then a *divides* b (equivalently: a is a *divisor* of b, or a is a *factor* of b) if there exists an integer c such that $b = ac$. If a divides b, then this is denoted by $a \mid b$.

Example 2 (i) $-3 \mid 18$, since $18 = (-3)(-6)$. (ii) $173 \mid 0$, since $0 = (173)(0)$.

The following are some elementary properties of divisibility.

Fact 3 (*properties of divisibility*) For all a, b, $c \in \mathbb{Z}$, the following are true:

(i) (*reflexivity*) $a \mid a$.

(ii) (*transitivity*) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(iii) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$.

(iv) If $a \mid b$ and $b \mid a$, then $a = \pm b$.

Definition 4 (*division algorithm for integers*) If a and b are integers with $b \geq 1$, then ordinary long division of a by b yields integers q (the *quotient*) and r (the *remainder*) such that

$$a = qb + r, \quad \text{where } 0 \leq r < b.$$

Moreover, q and r are unique. The remainder of the division is denoted $a \bmod b$.

Fact 5 Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then $a \bmod b = a - b\lfloor a/b \rfloor$.

Example 6 If $a = 73$, $b = 17$, then $q = 4$ and $r = 5$. Hence $73 \bmod 17 = 5$.

Definition 7 An integer c is a *common divisor* of a and b if $c \mid a$ and $c \mid b$.

Definition 8 A non-negative integer d is the *greatest common divisor* of integers a and b, denoted $d = \gcd(a, b)$, if

(i) d is a common divisor of a and b; and

(ii) whenever $c \mid a$ and $c \mid b$, then $c \mid d$.

Equivalently, $\gcd(a, b)$ is the largest positive integer that divides both a and b, with the exception that $\gcd(0, 0) = 0$.

Example 9 The common divisors of 12 and 18 are $\{\pm 1, \pm 2, \pm 3, \pm 6\}$, and $\gcd(12, 18) = 6$.

Definition 10 Two integers a and b are said to be *coprime* or *relatively prime* if $\gcd(a, b) = 1$.

Definition 11 An integer $p \geq 2$ is said to be *prime* if its only positive divisors are 1 and p. Otherwise, p is called *composite*.

The following are some well known facts about prime numbers.

Fact 12 (*Euclid's lemma*) If p is prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$ (or both).

Fact 13 (*Euclid's theorem*) There are infinitely many prime numbers.

Fact 14 (*fundamental theorem of arithmetic*) Every integer $n \geq 2$ has a factorization as a product of prime powers:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where the p_i are distinct primes and the e_i are positive integers. Furthermore, the factorization is unique up to rearrangement of factors.

Fact 15 If $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, where each $e_i \geq 0$ and $f_i \geq 0$, then

$$\gcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_k^{\min(e_k,f_k)}.$$

Example 16 Let $a = 4864 = 2^8 \cdot 19$, $b = 3458 = 2 \cdot 7 \cdot 13 \cdot 19$. Then $\gcd(4864, 3458) = 2 \cdot 19 = 38$.

The greatest common divisor of two integers a and b can be computed via Fact 15. However, computing a gcd by first obtaining prime-power factorizations does not result in an efficient algorithm, as the problem of factoring integers appears to be relatively difficult. The Euclidean algorithm (Algorithm 18) is an efficient algorithm for computing the greatest common divisor of two integers that does not require the factorization of the integers. It is based on the following simple fact.

Fact 17 If a and b are positive integers with $a > b$, then $\gcd(a,b) = \gcd(b, a \bmod b)$.

Algorithm 18 (Euclidean algorithm for computing the gcd of two integers)
INPUT: two non-negative integers a and b with $a \geq b$.
OUTPUT: the greatest common divisor of a and b.

```
1. While $b \neq 0$ do the following:
    1.1 Set $r \leftarrow a \bmod b$,  $a \leftarrow b$,  $b \leftarrow r$.
2. Return($a$).
```

Example 19 (*Euclidean algorithm*) The following are the division steps of Algorithm 18 for computing $\gcd(4864, 3458) = 38$:

$$\begin{aligned}
4864 &= 1 \cdot 3458 + 1406 \\
3458 &= 2 \cdot 1406 + 646 \\
1406 &= 2 \cdot 646 + 114 \\
646 &= 5 \cdot 114 + 76 \\
114 &= 1 \cdot 76 + 38 \\
76 &= 2 \cdot 38 + 0.
\end{aligned}$$

The Euclidean algorithm can be extended so that it not only yields the greatest common divisor d of two integers a and b, but also integers x and y satisfying $ax + by = d$.

Algorithm 20 (Extended Euclidean algorithm)
INPUT: two non-negative integers a and b with $a \geq b$.
OUTPUT: $d = \gcd(a, b)$ and integers x, y satisfying $ax + by = d$.

```
1. If $b = 0$ then set $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$, and return($d$,$x$,$y$).
2. Set $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$.
3. While $b > 0$ do the following:
   3.1 $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$.
   3.2 $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4. Set $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$, and return($d$,$x$,$y$).
```

Example 21 (*Extended Euclidean algorithm*) Table 1 shows the steps of Algorithm 20 with inputs $a = 4864$ and $b = 3458$. Hence $\gcd(4864, 3458) = 38$ and $(4864)(32) + (3458)(-45) = 38$.

q	r	x	y	a	b	x_2	x_1	y_2	y_1
–	–	–	–	4864	3458	1	0	0	1
1	1406	1	-1	3458	1406	0	1	1	-1
2	646	-2	3	1406	646	1	-2	-1	3
2	114	5	-7	646	114	-2	5	3	-7
5	76	-27	38	114	76	5	-27	-7	38
1	38	32	-45	76	38	-27	32	38	-45
2	0	-91	128	38	0	32	-91	-45	128

Table 1: Extended Euclidean algorithm (Algorithm 20) with inputs $a = 4864$, $b = 3458$.

2 The integers modulo n

Let n be a positive integer.

Definition 22 If a and b are integers, then a is said to be *congruent to b modulo n*, written $a \equiv b \pmod{n}$, if n divides $(a - b)$. The integer n is called the *modulus* of the congruence.

Example 23 (i) $24 \equiv 9 \pmod{5}$ since $24 - 9 = 3 \cdot 5$.
(ii) $-11 \equiv 17 \pmod{7}$ since $-11 - 17 = -4 \cdot 7$.

Fact 24 (*properties of congruences*) For all a, a_1, b, b_1, $c \in \mathbb{Z}$, the following are true.

(i) $a \equiv b \pmod{n}$ if and only if a and b leave the same remainder when divided by n.

(ii) (*reflexivity*) $a \equiv a \pmod{n}$.

(iii) (*symmetry*) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.

(iv) (*transitivity*) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

(v) (*congruences can be added and multiplied*) If $a \equiv a_1 \pmod{n}$ and $b \equiv b_1 \pmod{n}$, then $a + b \equiv a_1 + b_1 \pmod{n}$ and $ab \equiv a_1 b_1 \pmod{n}$.

The *equivalence class* of an integer a is the set of all integers congruent to a modulo n. From properties (ii), (iii), and (iv) above, it can be seen that for a fixed n the relation of congruence modulo n partitions $\mathbb{Z}$ into equivalence classes. Now, if $a = qn + r$, where $0 \leq r < n$, then $a \equiv r \pmod{n}$. Hence each integer a is congruent modulo n to a unique integer between 0 and $n - 1$, called the *least residue* of a modulo n. Thus a and r are in the same equivalence class, and so r may simply be used to represent this equivalence class.

Definition 25 The *integers modulo n*, denoted $\mathbb{Z}_n$, is the set of (equivalence classes of) integers $\{0, 1, 2, \ldots, n-1\}$. Addition, subtraction, and multiplication in $\mathbb{Z}_n$ are performed modulo n.

Example 26 $\mathbb{Z}_{25} = \{0, 1, 2, \ldots, 24\}$. In $\mathbb{Z}_{25}$, $13 + 16 = 4$ since $13 + 16 = 29 \equiv 4 \pmod{25}$. Similarly, $13 \cdot 16 = 8$ in $\mathbb{Z}_{25}$ since $13 \cdot 16 = 208 \equiv 8 \pmod{25}$.

Definition 27 Let $a \in \mathbb{Z}_n$. The *(multiplicative) inverse* of a modulo n is an integer $x \in \mathbb{Z}_n$ such that $ax \equiv 1 \pmod{n}$. If such an x exists, then it is unique, and a is said to be *invertible*; the inverse of a modulo n is denoted by $a^{-1} \bmod n$.

Definition 28 Let $a, b \in \mathbb{Z}_n$. *Division* of a by b modulo n, written $a/b \bmod n$, is the product of a and b^{-1} modulo n, and is only defined if b is invertible modulo n.

Fact 29 Let $a \in \mathbb{Z}_n$. Then a is invertible if and only if $\gcd(a, n) = 1$.

Example 30 The invertible elements in $\mathbb{Z}_9$ are 1, 2, 4, 5, 7, and 8. For example, $4^{-1} = 7$ because $4 \cdot 7 = 28 \equiv 1 \pmod{9}$. Also, 3 is not invertible in $\mathbb{Z}_9$ since there does not exist an integer x satisfying $3x \equiv 1 \pmod{9}$.

The following is a generalization of Fact 29.

Fact 31 Let $d = \gcd(a, n)$. The linear congruence $ax \equiv b \pmod{n}$ has a solution x if and only if d divides b, in which case there are exactly d solutions between 0 and $n - 1$; these solutions are all congruent modulo n/d.

If $\gcd(a, n) \mid b$, then a solution x to the linear congruence $ax \equiv b \pmod{n}$ can be found as follows:

(i) Use the Extended Euclidean algorithm to find integers x_0 and y_0 such that $ax_0 + ny_0 = d$, where $d = \gcd(a, n)$.

(ii) Then $x = x_0 b/d$.

Remark 32 (*computing inverses modulo n*) Let $a \in [1, n-1]$ and suppose that $\gcd(a, n) = 1$. By Fact 31, $a^{-1} \bmod n$ can be computed by using the Extended Algorithm algorithm to find integers x and y such that $ax + ny = 1$; then $a^{-1} = x \bmod n$.

Fact 33 (*Fermat's little theorem*) Let p be a prime. If $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. In other words, the remainder upon dividing a^{p-1} by p is 1.

Example 34 $p = 1299709$ is prime, so $12345^{1299708} \equiv 1 \pmod{1299709}$.

Remark 35 (*finding inverses modulo p*) Let p be a prime nunber. Then all nonzero elements $a \in \mathbb{Z}_p$, i.e., the integers in $\{1, 2, \ldots, p-1\}$, satisfy $\gcd(a, p) = 1$. Hence, all nonzero elements in $\mathbb{Z}_p$ are invertible. Fermat's little theorem gives an alternate method for finding inverses modulo p. Namely, if $a \in \{1, 2, \ldots, p-1\}$, then $a^{-1} = a^{p-2} \pmod{p}$. Justification: $a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p}$.

3 Exercises

1. Use the Euclidean algorithm to compute $\gcd(4071, 5133)$. [Answer: 177]
2. Find $3^{-1} \bmod 25$ by trial and error. [Answer: 17]
3. Compute $3/7 \bmod 11$. [Answer: 2]
4. Use the Extended Euclidean algorithm to compute $562^{-1} \bmod 1547$. [Answer: 256]
5. Solve $3x \equiv 19 \pmod{23}$. [Answer: $x \equiv 14 \pmod{23}$]
6. Use the definition of divisibility to prove the statements in Fact 3.
7. Use the definition of congruence modulo n to prove the statements in Fact 24.