CPSC 467: Cryptography and Security

Michael J. Fischer

Lecture 11
October 6, 2020

Number Theory for RSA

Modular Arithmetic
- Division of Integers

Integers Modulo n

Multiplicative Subgroup of $\mathbf{Z}_n$
- Greatest common divisor
- Multiplicative subgroup of $\mathbf{Z}_n$

Number Theory for RSA

Recall: RSA cryptosystem in a nutshell

RSA Step	**Number Theory Needed**
Choose two large primes p, q.	Primality test
$n = pq$ and $\phi(n) = (p-1)(q-1)$.	Bignum arithmetic
Choose e, d so $ed \equiv 1 \pmod{\phi(n)}$.	Diophantine equations
It follows that $m^{ed} \equiv m \pmod{n}$.	Euler's theorem
$\left.\begin{array}{l} E_e(m) = c = m^e \bmod n \\ D_d(c) = m = c^d \bmod n. \end{array}\right\}$	Fast modular exponentiation

Modular Arithmetic

$\mathbf{Z}_n$, $\mathbf{Z}_n^*$, and products of two primes

We first need

- Some theory of $\mathbf{Z}_n$, the integers modulo n;
- Some theory of $\mathbf{Z}_n^*$, the integers in $\mathbf{Z}_n$ that have no divisors in common with n (except for 1);
- The Euler *totient* function $\phi(n) = |\mathbf{Z}_n^*|$;
- Some properties of numbers n that are the product of two distinct large primes. In particular, for such numbers n, $\phi(n) = |\mathbf{Z}_n^*| = (p-1)(q-1)$.

Quotient and remainder

Theorem (Euclidean division)

Let a, b be integers and assume $b > 0$. There are unique integers q (the quotient) and r (the remainder) such that $a = bq + r$ and $0 \leq r < b$.

Write the quotient as $a \div b$ and the remainder as $a \bmod b$. Then

$$a = b \times (a \div b) + (a \bmod b).$$

Equivalently,

$$a \bmod b = a - b \times (a \div b).$$

$$a \div b = \lfloor a/b \rfloor.$$ [1]

[1] Here, / is ordinary real division and $\lfloor x \rfloor$, the *floor* of x, is the greatest integer $\leq x$. In C, / is used for both $\div$ and / depending on its operand types.

Divides

b divides a (exactly), written $b \mid a$, in case $a \equiv 0 \pmod{b}$ (or equivalently, $a = bq$ for some integer q).

Fact

If $d \mid (a+b)$, then either d divides both a and b, or d divides neither of them.

Proof.

Suppose $d \mid (a+b)$ and $d \mid a$. Then $a + b = dq_1$ and $a = dq_2$ for some integers q_1 and q_2. Substituting for a and solving for b, we get

$$b = dq_1 - dq_2 = d(q_1 - q_2).$$

Hence, $d \mid b$. $\square$

The mod operator for negative numbers

When either a or b is negative, there is no consensus on the definition of $a \bmod b$.

By our definition, $a \bmod b$ is always in the range $[0 \ldots b-1]$, even when a is negative.

Example,

$$(-5) \bmod 3 = (-5) - 3 \times ((-5) \div 3) = -5 - 3 \times (-2) = 1.$$

The mod operator % in C

In the C programming language, the mod operator % is defined differently, so $(a \,\%\, b) \neq (a \bmod b)$ when a is negative and b is positive.

The C standard defines $a \,\%\, b$ to be the number r satisfying the equation $(a/b) * b + r = a$, so $r = a - (a/b) * b$.

C also defines a/b to be the result of rounding the real number a/b towards zero, so $-5/3 = -1$. Hence,

$$-5 \,\%\, 3 = -5 - (-5/3) * 3 = -5 + 3 = -2.$$

Integers Modulo n

The mod relation

We just saw that mod is a binary operation on integers.

Mod is also used to denote a relationship on integers:

$$a \equiv b \pmod{n} \quad \text{iff} \quad n \mid (a - b).$$

That is, a and b have the same remainder when divided by n. An immediate consequence of this definition is that

$$a \equiv b \pmod{n} \quad \text{iff} \quad (a \bmod n) = (b \bmod n).$$

Thus, the two notions of mod aren't so different after all!

We sometimes write $a \equiv_n b$ to mean $a \equiv b \pmod{n}$.

Mod is an equivalence relation

The two-place relationship $\equiv_n$ is an *equivalence relation*.

The relation $\equiv_n$ partitions the integers $\mathbf{Z}$ into n pairwise disjoint infinite sets $C_0, \ldots, C_{n-1}$, called *residue classes*, such that:

1. Every integer is in a unique residue class;
2. Integers x and y are equivalent $\pmod{n}$ if and only if they are members of the same residue class.

Representatives for residue classes

The unique class C_j containing integer b is denoted by $[b]_{\equiv_n}$ or simply by $[b]$.

Fact

$$[a] = [b] \textit{ iff } a \equiv b \pmod{n}.$$

If $x \in [b]$, then x is said to be a *representative* or *name* of the residue class $[b]$. Obviously, b is a representative of $[b]$.

For example, if $n = 7$, then $[-11]$, $[-4]$, $[3]$, $[10]$, $[17]$ are all names for the same residue class

$$C_3 = \{\ldots, -11, -4, 3, 10, 17, \ldots\}.$$

Canonical names

The *canonical* or preferred name for the class $[b]$ is the unique representative x of $[b]$ in the range $0 \le x \le n-1$.

For example, if $n = 7$, the canonical name for $[10]$ is 3.

Why is the canonical name unique?

Mod is a congruence relation

Definition

The relation $\equiv$ is a *congruence relation* with respect to addition, subtraction, and multiplication of integers if

1. $\equiv$ is an equivalence relation, and
2. for each arithmetic operation $\odot \in \{+, -, \times\}$, if $a \equiv a'$ and $b \equiv b'$, then $a \odot b \equiv a' \odot b'$.

The class containing the result of $a \odot b$ depends only on the classes to which a and b belong and not the particular representatives chosen. Thus,

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

Operations on residue classes

We can extend our operations to work directly on the family of residue classes (rather than on integers).

Let $\odot$ be an arithmetic operation in $\{+, -, \times\}$, and let $[a]$ and $[b]$ be residue classes. Define $[a] \odot [b] = [a \odot b]$.

If you've followed everything so far, it should be no surprise that the canonical name for $[a \odot b]$ is $(a \odot b) \bmod n$!

Multiplicative Subgroup of $\mathbf{Z}_n$

Greatest common divisor

Definition

The *greatest common divisor* of two integers a and b, written $\gcd(a, b)$, is the largest integer d such that $d \mid a$ and $d \mid b$.

$\gcd(a, b)$ is always defined unless $a = b = 0$ since 1 is a divisor of every integer, and the divisor of a non-zero number cannot be larger (in absolute value) than the number itself.

Question: Why isn't $\gcd(0, 0)$ well defined?

Computing the GCD

$\gcd(a, b)$ is easily computed if a and b are given in factored form.

Namely, let p_i be the i^{th} prime. Write $a = \prod p_i^{e_i}$ and $b = \prod p_i^{f_i}$. Then

$$\gcd(a, b) = \prod p_i^{\min(e_i, f_i)}.$$

Example: $168 = 2^3 \cdot 3 \cdot 7$ and $450 = 2 \cdot 3^2 \cdot 5^2$, so $\gcd(168, 450) = 2 \cdot 3 = 6$.

However, factoring is believed to be a hard problem, and no polynomial-time factorization algorithm is currently known. (If it were easy, then Eve could use it to break RSA, and RSA would be of no interest as a cryptosystem.)

Euclidean algorithm

Fortunately, $\gcd(a, b)$ can be computed efficiently without the need to factor a and b using the famous *Euclidean algorithm*.

Euclid's algorithm is remarkable, not only because it was discovered a very long time ago, but also because it works without knowing the factorization of a and b.

Euclidean identities

The Euclidean algorithm relies on several identities satisfied by the gcd function. In the following, assume $a > 0$ and $a \geq b \geq 0$:

$$\begin{aligned} \gcd(a, b) &= \gcd(b, a) && (1) \\ \gcd(a, 0) &= a && (2) \\ \gcd(a, b) &= \gcd(a - b, b) && (3) \end{aligned}$$

Identity 1 is obvious from the definition of gcd. Identity 2 follows from the fact that every positive integer divides 0. Identity 3 follows from the basic fact relating divides and addition on slide 8.

Computing GCD without factoring

The Euclidean identities allow the problem of computing $\gcd(a, b)$ to be reduced to the problem of computing $\gcd(a - b, b)$.

The new problem is "smaller" as long as $b > 0$.

The *size* of the problem $\gcd(a, b)$ is $|a| + |b|$, the sum of the absolute value of the two arguments.

An easy recursive GCD algorithm

```
int gcd(int a, int b)
{
  if ( a < b ) return gcd(b, a);
  else if ( b == 0 ) return a;
  else return gcd(a-b, b);
}
```

This algorithm is not very efficient, as you will quickly discover if you attempt to use it, say, to compute $\gcd(1000000, 2)$.

Repeated subtraction

Repeatedly applying identity (3) to the pair (a, b) until it can't be applied any more produces the sequence of pairs

$$(a, b), (a - b, b), (a - 2b, b), \dots, (a - qb, b).$$

The sequence stops when $a - qb < b$.

How many times you can subtract b from a while remaining non-negative?
Answer: The quotient $q = \lfloor a/b \rfloor$.

Using division in place of repeated subtractions

The amout $a - qb$ that is left after q subtractions is just the remainder $a \bmod b$.

Hence, one can go directly from the pair (a, b) to the pair $(a \bmod b, b)$.

This proves the identity

$$\gcd(a, b) = \gcd(a \bmod b, b). \tag{4}$$

Full Euclidean algorithm

Recall the inefficient GCD algorithm.

```
int gcd(int a, int b) {
  if ( a < b ) return gcd(b, a);
  else if ( b == 0 ) return a;
  else return gcd(a-b, b);
}
```

The following algorithm is exponentially faster.

```
int gcd(int a, int b) {
  if ( b == 0 ) return a;
  else return gcd(b, a%b);
}
```

Principal change: Replace `gcd(a-b,b)` with `gcd(b, a%b)`.

Besides collapsing repeated subtractions, we have $a \geq b$ for all but the top-level call on $\gcd(a, b)$. This eliminates roughly half of the remaining recursive calls.

Complexity of GCD

The new algorithm requires at most in $O(n)$ stages, where n is the sum of the lengths of a and b when written in binary notation, and each stage involves at most one remainder computation.

The following iterative version eliminates the stack overhead:

```
int gcd(int a, int b) {
  int aa;
  while (b > 0) {
    aa = a;
    a = b;
    b = aa % b;
  }
  return a;
}
```

Relatively prime numbers

Two integers a and b are *relatively prime* if they have no common prime factors.

Equivalently, a and b are *relatively prime* if $\gcd(a, b) = 1$.

Let $\mathbf{Z}_n^*$ be the set of integers in $\mathbf{Z}_n$ that are relatively prime to n, so

$$\mathbf{Z}_n^* = \{a \in \mathbf{Z}_n \mid \gcd(a, n) = 1\}.$$

Example:

$$\mathbf{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}.$$

Euler's totient function $\phi(n)$

$\phi(n)$ is the cardinality (number of elements) of $\mathbf{Z}_n^*$, i.e.,

$$\phi(n) = |\mathbf{Z}_n^*|.$$

Example: $\phi(21) = |\mathbf{Z}_{21}^*| = 12.$

Go back and count them!

Properties of $\phi(n)$

1. If p is prime, then
$$\phi(p) = p - 1.$$
2. More generally, if p is prime and $k \geq 1$, then
$$\phi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}.$$
3. If $\gcd(m, n) = 1$, then
$$\phi(mn) = \phi(m)\phi(n).$$

Example: $\phi(126)$

Can compute $\phi(n)$ for all $n \geq 1$ given the factorization of n.

$$\begin{aligned} \phi(126) &= \phi(2) \cdot \phi(3^2) \cdot \phi(7) \\ &= (2-1) \cdot (3-1)(3^{2-1}) \cdot (7-1) \\ &= 1 \cdot 2 \cdot 3 \cdot 6 = 36. \end{aligned}$$

The 36 elements of $\mathbf{Z}_{126}^*$ are:

1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41, 43, 47, 53, 55, 59, 61, 65, 67, 71, 73, 79, 83, 85, 89, 95, 97, 101, 103, 107, 109, 113, 115, 121, 125.

A formula for $\phi(n)$

Here is an explicit formula for $\phi(n)$.

Theorem

Write n in factored form, so $n = p_1^{e_1} \cdots p_k^{e_k}$, where $p_1, \ldots, p_k$ are distinct primes and $e_1, \ldots, e_k$ are positive integers.[2] *Then*

$$\phi(n) = (p_1 - 1) \cdot p_1^{e_1 - 1} \cdots (p_k - 1) \cdot p_k^{e_k - 1}.$$

Important: For the product of distinct primes p and q,

$$\phi(pq) = (p-1)(q-1).$$

[2] By the fundamental theorem of arithmetic, every integer can be written uniquely in this way up to the ordering of the factors.