Number theory (Chapter 4)

Review

If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When a divides b we say that a is a *factor* or *divisor* of b, and that b is a *multiple* of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \qquad \text{and} \qquad ac \equiv bd \pmod{m}.$$

Let m be a positive integer and let a and b be integers. Then

$$(a + b) \mathbf{~mod~} m = ((a \mathbf{~mod~} m) + (b \mathbf{~mod~} m)) \mathbf{~mod~} m$$

and

$$ab \mathbf{~mod~} m = ((a \mathbf{~mod~} m)(b \mathbf{~mod~} m)) \mathbf{~mod~} m.$$

Questions:

1. Does 5|1? Does 1|5?
2. Does (129+63) mod 10 = (129 mod 10)+(63 mod 10)?
3. Does (129+63) mod 10 = ((129 mod 10)+(63 mod 10)) mod 10?
4. How could you quickly find (69*40) mod 6?

Quiz tomorrow includes chapter 3, section 4.1 and only up to page 249 of section 4.2. You should certainly be comfortable with the above theorems…

Modular Exponentiation

In cryptography it is important to be able to find b^n **mod** m efficiently, where b, n, and m are large integers. It is impractical to first compute b^n and then find its remainder when divided by m because b^n will be a huge number. Instead, we can use an algorithm that employs the binary expansion of the exponent n.[i]

OK, this gets tricky. What we are going to do is notice that if we raise some number b to the n^{th} power, we can consider the binary representation of n as $(a_{k-1}, \ldots a_1, a_0)$. So if n=12 we could consider 1100_2. Consider the claim that

$$b^n = b^{a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0} = b^{a_{k-1} \cdot 2^{k-1}} \cdots b^{a_1 \cdot 2} \cdot b^{a_0}.$$

[i] Text from page 253 of Rosen

In our case (n=12) we are saying that $b^{12}=b^8*b^4$ which is clearly true.

So what are going to do is take advantage of this

procedure *modular exponentiation*(b: integer, $n = (a_{k-1}a_{k-2}\dots a_1a_0)_2$,
m: positive integers)
$x := 1$
$power := b$ **mod** m
for $i := 0$ **to** $k-1$
  if $a_i = 1$ **then** $x := (x \cdot power)$ **mod** m
  $power := (power \cdot power)$ **mod** m
return $x\{x$ equals b^n **mod** $m\}$

EXAMPLE 12 Use Algorithm 5 to find 3^{644} **mod** 645.

Solution: Algorithm 5 initially sets $x = 1$ and $power = 3$ **mod** $645 = 3$. In the computation of 3^{644} **mod** 645, this algorithm determines 3^{2^j} **mod** 645 for $j = 1, 2, \dots, 9$ by successively squaring and reducing modulo 645. If $a_j = 1$ (where a_j is the bit in the jth position in the binary expansion of 644, which is $(1010000100)_2$), it multiplies the current value of x by 3^{2^j} **mod** 645 and reduces the result modulo 645. Here are the steps used:

$i = 0$: Because $a_0 = 0$, we have $x = 1$ and $power = 3^2$ **mod** $645 = 9$ **mod** $645 = 9$;
$i = 1$: Because $a_1 = 0$, we have $x = 1$ and $power = 9^2$ **mod** $645 = 81$ **mod** $645 = 81$;
$i = 2$: Because $a_2 = 1$, we have $x = 1 \cdot 81$ **mod** $645 = 81$ and $power = 81^2$ **mod** $645 = 6561$ **mod** $645 = 111$;
$i = 3$: Because $a_3 = 0$, we have $x = 81$ and $power = 111^2$ **mod** $645 = 12{,}321$ **mod** $645 = 66$;
$i = 4$: Because $a_4 = 0$, we have $x = 81$ and $power = 66^2$ **mod** $645 = 4356$ **mod** $645 = 486$;
$i = 5$: Because $a_5 = 0$, we have $x = 81$ and $power = 486^2$ **mod** $645 = 236{,}196$ **mod** $645 = 126$;
$i = 6$: Because $a_6 = 0$, we have $x = 81$ and $power = 126^2$ **mod** $645 = 15{,}876$ **mod** $645 = 396$;
$i = 7$: Because $a_7 = 1$, we find that $x = (81 \cdot 396)$ **mod** $645 = 471$ and $power = 396^2$ **mod** $645 = 156{,}816$ **mod** $645 = 81$;
$i = 8$: Because $a_8 = 0$, we have $x = 471$ and $power = 81^2$ **mod** $645 = 6561$ **mod** $645 = 111$;
$i = 9$: Because $a_9 = 1$, we find that $x = (471 \cdot 111)$ **mod** $645 = 36$.

This shows that following the steps of Algorithm 5 produces the result 3^{644} **mod** $645 = 36$.

Let's see how we'd use this to find 5^{13} mod 3 (something a bit less painful).

On primes and greatest common divisors (4.3)

Chapter 4.3 does a lot with primes, and we're going to only hang around for some of the highlights. Let's start with the definition of prime and composite.

An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

And once we have that, we get something that is quite important (as the name may hint…)

THE FUNDAMENTAL THEOREM OF ARITHMETIC Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

In some ways that's self-evident. By definition of prime, you can't factor a prime number. And it seems reasonable to think that if a number is divisible by a certain prime, that prime must show up in the prime factorization. But we'll prove this theorem later as a nice example of strong induction (section 5.2)

1. What is the prime factorization of 100?
2. What is the prime factorization of 333?
3. What is the prime factorization of 1000?
4. What is the prime factorization of 370?

Greatest common divisor and least common multiples

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Questions

1. What is the gcd(100, 30)?
2. What is the gcd(100, 10)?
3. What is the gcd(333, 6)?
4. What is the gcd(40, 27)?
5. What is the gcd(27,0)?
6. What is the gcd of (333, 370)? ← use the answers from the prime factorizations found above…

The integers a and b are *relatively prime* if their greatest common divisor is 1. [ii]

Which of the above pairs are relatively prime?

[ii] Two numbers that are relatively prime are sometimes called *coprime.*

The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\mathrm{lcm}(a, b)$.

Questions

1. What is the lcm(100, 30)?
2. What is the lcm (100, 10)?
3. What is the lcm (333, 6)?
4. What is the lcm (40, 27)?
5. What is the lcm of (333, 370)? ← use the answers from the prime factorizations found above…

How are lcm and gcd related?

The Euclidean Algorithm

We are going to propose a fast way of finding the gcd of two numbers. Clearly, if we find the prime factorization of two numbers we can find the gcd by finding the common terms. But that may not be fast enough. Euclid proposed an algorithm that is much faster than searching for all factors (which in the worst case could take quite a while). Let's start by proving the following:

Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

OK, this is basically saying that if there is any factor which divides a and b, it must also divide r. So let's say that some factor "d" divides a and b. In that case, d also divides bq[iii]. And because r=a-bq, where d divides a and bq, it must also divide r. So any number (including the greatest one) that divides a and b must also divide r.

For example consider finding the gcd(30,12). This means that gcd(30,12)=gcd(30 mod 12, 12)=gcd(6,12)=6.

[iii] If a|b then $\forall d \in \aleph$, a|bd.

Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 & 0 \leq r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3 & 0 \leq r_3 < r_2,\\
&\ \ \vdots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1},\\
r_{n-1} &= r_n q_n.
\end{aligned}$$

Eventually a remainder of zero occurs in this sequence of successive divisions, because the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \geq 0$ cannot contain more than a terms. Furthermore, it follows from Lemma 1 that

$$\begin{aligned}
\gcd(a, b) &= \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1})\\
&= \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.
\end{aligned}$$

Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.

Find the gcd(255,300) using the Euclidian Algorithm.

index i	quotient q_{i-1}	Remainder r_i
0		300
1		255
2		
3		
4		
5		

We are now going to work on 4 key results we'll use for RSA.

- **Bezout's theorem** which states that $\forall ab\ \exists st\ sa + bt = \gcd(a, b)$
- **The definition of an inverse of a modulo m and a proof that it exists if a and m are relatively prime** That is, that ∀a∀(m>1)[gcd(a,m)=1 → ∃x(ax≡1 (mod m))]
- **Chinese remainder theorem** which states that if you've a group of relatively prime positive integers greater than 1 then you can count to the product of those primes in a unique way just using those primes (this one is actually easy, just hard to state succinctly).
- **Fermat's Little Theorem** which states if p is prime and a is not divisible by p then $a^{p-1} \equiv 1\ (mod\ p)$

(It is unlikely we will manage all 4 of these today, we'll finish/review on Thursday).

BÉZOUT'S THEOREM If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

At first glance, this seems quite reasonable, after all, for any a, b, can't we find integers s and t that are equal to *any* number? And the answer is no. Consider a=2 and b=4. You can find integers that get to any even number, but not any odd. And for those values of a and b, that's exactly what the theory says.

1. Find an s and t for a=9 and b=6 so that 9s+6t=gcd(9,6).

2. Find an s and t for a=5 and b=25

The general proof for this is by construction. The construction is called the "Extended Euclidean Algorithm[iv]". The EEA proceeds in the same way, but adds two sequences s_n and t_n as shown on the right.

Consider the input case of 252, 198. Let's first find the gcd.

[iv] https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm uses a less intuitive scheme but includes a proof.

Definition of a modulo inverse and statement of its existence (4.4)

If ax≡1 (mod m) then x is said to be an inverse of a modulo m. The claim below is that if a and m are relatively prime such an inverse exists and is unique modulo m.

If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (That is, there is a unique positive integer $\overline{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\overline{a}$ modulo m.)

(This proof shows existence, not uniqueness)

We know that gcd(a,m)=1, so from Bezout's theorem we know that ∃s,t as+mt=1.

Thus sa+tm≡1 (mod m). (Finish the proof below, it's just one or two more lines, though we won't show the uniqueness part.

1. Find the inverse of 7 modulo 12.

FERMAT'S LITTLE THEOREM If p is prime and a is an integer not divisible by p, then

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

Furthermore, for every integer a we have

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

We'll use this one without proof as all known proofs are fairly ugly. But see https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_little_theorem for some proofs if you are interested.

1. Pick some values a and p which meet the requirements above. Does the theorem hold?
2. Use Fermat's Little Theorem to find 7^{222} mod 11.

Chinese Remainder Theorem (4.4)

THE CHINESE REMAINDER THEOREM Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1},\\
x &\equiv a_2 \pmod{m_2},\\
&\ \ \vdots\\
x &\equiv a_n \pmod{m_n}
\end{aligned}
$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

These looks complex, but really it isn't. Let's do a group exercise and have one group be "mod 2" one group be "mod 3" and one group be "mod 5". This theorem says that if we count up to 30 (2*3*5) and each group counts by their mod (so mod 2 counts as 0,1,0,1, etc.) then we can count from 0 to 29 before there is a repeat.

We'll prove this a bit differently than the text does. We are trying to show that there is a unique solution. First let's define this scheme as a function *f* that maps from a domain m to a co-domain of m_1, m_2, …, m_n to m. Notice that the cardinality of the domain and co-domain are identical (m). Now let's assume there are two values a and b that generate the same values in the co-domain. In that case, a-b must each be divisible by all values of m_i. And as such, since each of the m's are relatively prime, it must be divisible by their product. But that's impossible as $|a-b|<m$ as a and b are both between 0 and m-1. Thus there are no two that have the same mapping (the function is one-to-one). And because they have the same cardinality, the function is also onto. It is thus a bijection and every instance in the domain maps to a unique instance in the co-domain. Done.

1. If we are using the values 2, 3, and 5 for m_1, m_2, m_3, what values of "a" would x=6 generate?
2. If we are using those same values, what is x if $a_1=1$, $a_2=2$, and $a_3=1$?