

1 Where we're headed

Ultimately, we'll look at a bit of cryptography as a non-trivial use of the “mod” function. We'll start with a bit of definition review and progress through some mathematical properties involving “mod”. Along the way, we'll point out some other computer science uses of this math.

2 Modular arithmetic and properties

2.1 Some starting definitions (mostly review)

- Definition: $a|b$: “a divides b”

Theorem 1: $a|b, a|c \rightarrow a|(b+c)$, for all $a, b, c \in Z$.

Proof: $a|b$ means $b = ax$, and $a|c$ means $c = ay$. So, $b+c = ax+ay = a(x+y)$, or equivalently, $a|(b+c)$.

Corollary 2: $a|b, a|c \rightarrow a|(b-c)$, for all $a, b, c \in Z$.

- For a base d , any integer a can be written $a = qd + r$ where $0 \leq r < d$. The quotient $q = a \text{ div } m$. The remainder $r = a \text{ mod } m$.

E.g., $5 \text{ mod } 3 = 8 \text{ mod } 3$, or $5 \text{ mod } 3 = 2$.

- Just defined “mod” as a binary function. Also common to use “mod” as a ternary relation: $5 \equiv 8 \pmod{3}$, or $5 \equiv 2 \pmod{3}$.

Q: What is a definition of the “mod” relation in terms of the “divides” relation?

A: $a \equiv b \pmod{m}$ iff $m|(a-b)$.

We will switch freely between the function and relation forms.

- Modular equivalence, for a given m , is truly an equivalence relation.

1. Verify: reflexive, symmetric, transitive
2. It partitions the universe into equivalence classes.

2.2 Modular addition

How does “mod” interact with other math operators? Let's start with addition.

Theorem 3: If $a \equiv a' \pmod{m}$, and $b \equiv b' \pmod{m}$, then $a+b \equiv a'+b' \pmod{m}$, for all $m \in Z^+, a, b, a', b' \in Z$.

Proof: $a' = im + a$, and $b' = jm + b$. So, $(a'+b') \text{ mod } m = ((i+j)m + (a+b)) \text{ mod } m = (a+b) \text{ mod } m$.

Corollary 4: $(a+b) \text{ mod } m = ((a \text{ mod } m) + (b \text{ mod } m)) \text{ mod } m$.

Proof: Let $a' = a \text{ mod } m$, $b' = b \text{ mod } m$ in the previous theorem.

2.3 Modular multiplication

We have a similar theorem to above:

Theorem 5: If $a \equiv a' \pmod{m}$, and $b \equiv b' \pmod{m}$, then $ab \equiv a_0b_0 \pmod{m}$, for all $m \in \mathbb{Z}^+$, $a, b, a', b' \in \mathbb{Z}$.

Proof: $a' = im + a$, and $b' = jm + b$. So, $a'b' \pmod{m} = ijm^2 + ajm + bim + ab = (ijm + aj + bi)m + ab$.

Corollary 6: $(ab) \pmod{m} = ((a \pmod{m})(b \pmod{m})) \pmod{m}$.

Proof: Let $a' = a \pmod{m}$, $b' = b \pmod{m}$ in the previous theorem.

Corollary 7: $a \equiv a' \pmod{m} \rightarrow a^k \equiv a'^k \pmod{m}$, for all $m \in \mathbb{Z}^+$, $a, a' \in \mathbb{Z}, k \in \mathbb{N}$.

Proof: By the previous theorem and induction.

2.4 Relatively prime

Definition: If $\gcd(a, b) = 1$, then a and b are *relatively prime* (or *coprime*).

2.5 Modular division

Theorem 8: If $ab \equiv ac \pmod{m}$, and $\gcd(a, m) = 1$, then $b \equiv c \pmod{m}$.

Example: $3x \equiv 15 \pmod{8}$ implies $x = 5$.

Non-example: $12 \equiv 4 \pmod{8}$ doesn't imply $3 \equiv 1 \pmod{8}$.

Proof: There exists i such that $im = ab - ac = a(b - c)$. Since im is divisible by a , and a and m are relatively prime, then i is divisible by a : $i = ja$. Thus, $jm = b - c$, and the conclusion holds.

Applications: parity check; hash functions

2.6 Modular Multiplicative Inverses

Consider the series $0a \pmod{m}$, $1a \pmod{m}$, $2a \pmod{m}$, $3a \pmod{m}$, $4a \pmod{m}$, \dots

Try $a = 5, m = 8$:

i	0	1	2	3	4	5	6	7	8	9	10	11	...
ia	0	5	10	15	20	25	30	35	40	45	50	55	...
$ia \pmod{m}$	0	5	2	7	4	1	6	3	0	5	2	7	...

We see we hit a cycle (of length 8).

Q: Why are we guaranteed to have a cycle?

A: $ia \pmod{m}$ only has m possible values – must repeat within $i = 0 \dots m$. After one repeated value, the rest must continue to repeat.

Q: What is $5^{-1} \pmod{8}$? I.e., the multiplicative inverse of 5, mod 8?

A: 5, since $5 \times 5 \equiv 1 \pmod{8}$, so 5 is its own inverse: $5^{-1} \equiv 5 \pmod{8}$.

Try $a = 6, m = 8$:

i	0	1	2	3	4	5	6	...
ia	0	6	12	18	24	30	36	...
$ia \bmod m$	0	6	4	2	0	6	4	...

Again, we have a cycle.

Q: What is $6^{-1} \pmod{8}$?

A: It doesn't exist! (6 times any number is even, and not 1 plus a multiple of 8.)

Q: Why does 5 have an inverse mod 8, and 6 doesn't?

A: 5 is relatively prime to 8. a has a multiplicative inverse mod m if and only if $\gcd(a, m) = 1$.

Proof of "if": (Omitted, but follows from Euclid's GCD algorithm below.)

Proof of "only if": If a has a multiplicative inverse mod m , then there exists x (the inverse) and k such that $km = ax - 1$. Let $j = \gcd(a, m)$, so $a = a'j$, $m = m'j$. Then $km'j = a'jx - 1$, or equivalently, $j(a'x - km') = 1$. Since everything is integral, j must be 1.

3 Encryption and Keys

What is encryption? Adam has a message M for Betty. Adam encrypts the message into E , and transmits this message. Betty receive this encrypted form, and decrypts it into D . We want $D = M$.

Traditionally, encryption relied upon a shared secret. Adam and Betty use the same knowledge – given either algorithm, you can figure out the other. A standard example is the *simple substitution cipher*. the consistent substitution of one letter for another (i.e., a bijection from and to the alphabet).

Two concerns:

- How do Adam and Betty come to share their secret? Can't initially send in encrypted form, since they don't yet share a secret. The secret must be sent unencrypted, and anyone who sees the message will also have the secret.

We would prefer a system in which the secret is not shared.

- Many older encryption methods are relatively easy to break, given access to just encrypted messages. E.g., for simple substitution cyphers, there are $26!$ or $52!$ possible bijections. That's too large for just brute-force, but we can incorporate knowledge about the frequency of letters, letter combinations, and word sizes in English to help tremendously.

3.1 Public-Key Encryption

Adam and Betty use well-known public algorithms, but with specific key data. One has a public key, and one a private (secret) key. The keys are paired – a specific encryption key uses a specific decryption key.

There are two variants:

- The encryption key is public. Thus, anyone can encrypt a message. But, since Betty's decryption key is private, the messages are only readable by Betty.
- The decryption key is public. Thus, anyone can decrypt the messages. But, since Adam's encryption key is private, the messages are effectively "signed" by Adam.

We'll concentrate on the first, but the math is the same for both. It is possible to combine these two advantages, by encoding a message twice, which two pairs of keys.

4 A Simple Public-Key Scheme

Our public encryption algorithm is $E = e \cdot M \bmod m$. The public key is the pair $\langle e, m \rangle$. Thus, M must be in $\{0, \dots, m\}$.

We will use $e = 37$, $m = 100$.

Examples – students give encrypted messages.

Our decryption algorithm is $D = d \cdot E \bmod m$, where $\langle d, m \rangle$ is the private key.

Here, $d = 73$, and $m = 100$ still.

4.1 Breaking the Simple Scheme

Q: How can you try to discover the private key?

A: Encrypt each of the $m = 100$ possible messages, and compare to the given message.

A: Given e, m , find $d = e^{-1} \bmod m$ by building a table, as above.

A: Given e, m , find $d = e^{-1} \bmod m$ by trying values $0, \dots, m - 1$.

A: Given e, m , find $d = e^{-1} \bmod m$ by writing, e.g., $37d = 1 + 100x$, and thus $d = (1 + 100x)/37$. To ensure $d < 100$, we need only try $x < 37$.

Each of these options are linear in the public key: $\langle 37, 100 \rangle$.

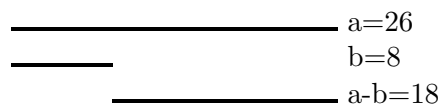
Q: Is linear good enough?

A: Yes, if we use really big keys, e.g., a couple hundred bits.

Alas, we can find multiplicative inverses in *logarithmic* time. We modify Eulid's gcd (greatest common divisor) algorithm (circa 300 B.C.E.).

Claim: $\gcd(a, b) = \gcd(b, a - b)$ (if $a > b$).

Think of a and b as lengths, and their gcd as the longest ruler which evenly measures both.



In the process of evenly measuring a , the gcd must also evenly measure b . Thus, it must evenly measure what's left of a , i.e., $a - b$.

Further claim: $\gcd(a, b) = \gcd(b, \text{remainder}(a, b))$ (if $a > b$).

Similar to before:



$$\begin{array}{r}
 \text{-----} \\
 \text{-----} \\
 \text{--- rem(a,b)=2}
 \end{array}
 \quad
 \begin{array}{l}
 b=8 \\
 3b=24
 \end{array}$$

In the process of evenly measuring a , the gcd must also evenly measure b , as well as any multiple of b . Thus, it must evenly measure what's left of a after any multiple of b , including the remainder of a and b .

Q: What is $\text{gcd}(n, 0)$?

A: n

Euclid's gcd algorithm:

```
(define (gcd a b)
  (if (zero? b)
      a
      (gcd b (remainder a b))))
```

Let's use the algorithm to compute $\text{gcd}(100, 37)$. Keeping track of remainders and quotients will eventually get us to our goal of finding $37^{-1} \pmod{100}$.

$$\begin{array}{ll}
 100 = 37 * 2 + 26 & \text{so } \text{gcd}(100, 37) = \text{gcd}(37, 26) \\
 37 = 26 * 1 + 11 & \text{so } \text{gcd}(37, 26) = \text{gcd}(26, 11) \\
 26 = 11 * 2 + 4 & \text{so } \text{gcd}(26, 11) = \text{gcd}(11, 4) \\
 11 = 4 * 2 + 3 & \text{so } \text{gcd}(11, 4) = \text{gcd}(4, 3) \\
 4 = 3 * 1 + 1 & \text{so } \text{gcd}(4, 3) = \text{gcd}(3, 1) \\
 3 = 1 * 3 + 0 & \text{so } \text{gcd}(3, 1) = \text{gcd}(1, 0) = 1
 \end{array}$$

Now rewrite those equations in a different form:

$$\begin{array}{l}
 1 = 4 - 1 * 3 \\
 3 = 11 - 2 * 4 \\
 4 = 26 - 2 * 11 \\
 11 = 37 - 1 * 26 \\
 26 = 100 - 2 * 37
 \end{array}$$

And now replace corresponding terms by the following equation:

$$\begin{array}{ll}
 1 = 4 - 1 * 3 & 1 = 4 - 1 * 3 \\
 3 = 11 - 2 * 4 & = 4 - 1 * (11 - 2 * 4) = -11 + 3 * 4 \\
 4 = 26 - 2 * 11 & = -11 + 3 * (26 - 2 * 11) = 3 * 26 - 7 * 11 \\
 11 = 37 - 1 * 26 & = 3 * 26 - 7 * (37 - 1 * 26) = -7 * 37 + 10 * 26 \\
 26 = 100 - 2 * 37 & = -7 * 37 + 10 * (100 - 2 * 37) = 10 * 100 - 27 * 37
 \end{array}$$

At the end, $1 = 10 * 100 - 27 * 37$, and thus $-27 * 37 \equiv 1 \pmod{100}$. So, $37^{-1} \pmod{100} = -27 \pmod{100} = 73$.

5 More modular arithmetic properties

Review:

- $a \equiv b \pmod{m}$ iff $a - b = xm$ for some $x \in \mathbb{Z}$.
- If $\text{gcd}(a, m) = 1$, then $a^{-1} \pmod{m}$ exists and can be efficiently computed.

5.1 Fermat's Little Theorem

Let p be prime, and a be relatively prime to p . Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: Let $S = \{1, 2, 3, \dots, p-1\}$. Let $T = \{a \bmod p, 2a \bmod p, 3a \bmod p, \dots, a(p-1) \bmod p\}$. We will show these two sets are identical, i.e., have the same numbers. So their products mod p are equal: $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$. Since $(p-1)!$ is relatively prime to p , we can divide, obtaining $1 \equiv a^{p-1} \pmod{p}$.

Clearly each element of T is in the range $0, \dots, p-1$. Let's see why 0 isn't in T . For $ka \bmod p$ to be 0, then $p|ka$ must be true. But that can't hold since both a and k are relatively prime to p by assumption, and k since it is in the range $1, \dots, p-1$ for the prime p .

Thus T is a subset of S . To show equality, it is sufficient to show that each element in T is unique. If there are no duplicates in the $p-1$ formulas for T 's elements, then there must be $p-1$ elements, which must be $1, \dots, p-1$.

Suppose they aren't unique, i.e., there are some $r, s \in \{1, \dots, p-1\}$ such that $r \neq s$, but $ra \equiv sa \pmod{p}$. Since a and p are relatively prime, we can divide by a : $r \equiv s \pmod{p}$. Thus $r = s + xp$ for some x . But r is between 0 and $p-1$, so $x = 0$. So $r = s$, and we assumed otherwise. Contradiction.

Historical Aside: This was posed in 1640: "(And this proposition is generally true for all progressions and for all prime numbers; the proof of which I would send to you, if I were not afraid that it would be too long.)" Around 1680 Leibniz proved it, but evidently decided that it wasn't important enough to publish and so his proof wasn't discovered until after Euler, a hundred years after it was stated, finally proved it.

Further aside: Fermat wasn't actually a mathematician. He was a lawyer, and occasionally had to be an appeals judge in high-profile cases. He took his neutrality *so* seriously that he didn't want to socialize with his peers, lest he become biased in his job. So he took up mathematics as a way to avoid having a social life.

5.2 Chinese Remainder Theorem Corollary

Sun-Tzu posed the question, "Suppose we have an unknown number of objects. When counted in threes, 2 are left over, when counted in fives, 3 are left over, and when counted in sevens, 2 are left over. How many objects are there?" He then proceeds to answer the question, in the process sketching the proof that doing arithmetic mod $3 \cdot 5 \cdot 7$ is the same as doing three simpler arithmetic problems in parallel (one mod 3, another mod 5, and another mod 7).

We won't prove the Chinese Remainder Theorem here (see book if interested), but we need a corollary:

If $\gcd(m, n) = 1$, $x \equiv a \pmod{m}$, and $x \equiv a \pmod{n}$, then $x \equiv a \pmod{mn}$.

Proof of corollary: We know that $x = a + im$, and $x = a + jn$, for some $i, j \in \mathbb{Z}$. Thus $im = jn$. Since everything is integral, im must be divisible by n , but since m and n are relatively prime, it must be i that is divisible by n . I.e., $i = kn$ for some $k \in \mathbb{Z}$. Thus $x = a + knm$, or equivalently, $x \equiv a \pmod{mn}$.

6 A Better Public-Key Scheme – RSA

This is similar to our simple scheme, only a little more complicated, but much more secure. (Most of the additional complication is in proving security and correctness, not in the algorithm.) Due to

Rivest, Shamir, Adleman (1977).

6.1 The Keys

- Find large primes (say, 200 digits) p, q .

There are known ways that we won't look at. That primes being fairly common helps us.

- Compute $m = pq$.
- Find e that is relatively prime to $(p - 1)(q - 1)$.
- Compute $d = e^{-1} \bmod (p - 1)(q - 1)$.

If anyone finds out p and q , they can compute $(p - 1)(q - 1)$, and since e is public, they can find d . More on this later.

6.2 Sending messages

Encryption: $E = M^e \bmod m$. Decryption: $D = E^d \bmod m$.

6.3 Correctness

We need to verify that $D = M$. Clearly, $D = M^{ed} \bmod m$. Recall that e and d are multiplicative inverses – mod $(p - 1)(q - 1)$, not mod m . But it does mean $ed = 1 + x(p - 1)(q - 1)$.

$$D = M^{ed} \bmod m = M^{1+x(p-1)(q-1)} \bmod m.$$

Let's look at this mod p , for a moment.

$$D = M^{1+x(p-1)(q-1)} \equiv M \cdot M^{x(p-1)(q-1)} \equiv M \cdot (M^{p-1})^{x(q-1)} \pmod{p}.$$

Now, by Fermat's Little Theorem, we have $M^{p-1} \equiv 1 \pmod{p}$. Thus,

$$D \equiv M \cdot 1^{x(q-1)} \equiv M \pmod{p}.$$

Similarly, $D \equiv M \pmod{q}$.

So, by the Chinese Remainder Theorem corollary, $D \equiv M \pmod{m}$. And since D and M are both in the range $0 \dots m - 1$, then $D = M$, as desired.

6.4 Attacks

If an eavesdropper can determine p, q , then they can break RSA. How difficult is it to factor the public m ?

If m is, say, a 400-digit number, there are 10^{400} potential divisors, or if you use primes, about $10^{400}/400 \ln(10) \approx 10^{397}$ divisors. How long, at 10^{10} divisions/sec?

Is there a better way to factor? *We don't know.*

6.5 Finding Large Primes

How common are primes? Certainly, their distribution is a bit sporadic, but as numbers get bigger they seem to become more sparse. Let $P(n)$ denote the number of primes less than n . A crown jewel of Number Theory is

$$P(n) \approx n/\ln(n).$$

(This is a simplification.)

So, how many 100-digit numbers are prime? About one in 300! (By comparison, how many 100-digit numbers are perfect squares? Out of the first 10^{100} numbers, only 10^{50} are, which is a miniscule fraction!) Primes are pretty common! By choosing 100-digit numbers at random, a computer is almost sure to find one within a few hundred iterations.

However, this brings up a different question: if a computer guesses a number, can it (quickly) know whether the number is prime? Alas, doing 10^{100} attempted divisions doesn't count as "quick". Interestingly, testing primality seems easier than factoring – see "Miller's Test" in the book for one (probabilistic) algorithm. People have also recently found a non-randomized asymptotically-quick algorithm for testing primality, but it is empirically slower than the randomized tests.

7 Some Final Thoughts on Number Theory

We are covering a very specific branch of number theory, modular arithmetic. We are dealing with all sorts of interesting things that come out of two numbers which happen to be relatively prime. But do not think that this is a unique relation: there is something interesting about almost every number. The best story of this is when Ramunajan, an absolute mathematical genius, was in the hospital and visited by Hardy. Hardy noted that the number on the door, "1729" and remarked that the number seemed to me rather a dull one, and that he hoped it was not an unfavorable omen. Ramunajan replies, "No, it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways."

In fact, it is also the first occurrence of all ten digits consecutively in the decimal representation of e .

It's also a Carmichael Number, an odd composite number which satisfies Fermat's Little Theorem, i.e., a pseudoprime relative to *every* base. The first three Carmichael Numbers are 561, 1105, and 1729.

Feynman story: Finally the Japanese man calls out "Raios cubicos!" – he wants to challenge Feynman to cube roots. Feynman says the man wrote a number, "any old number", down on a piece of paper, and he still remembers the number . . . 1729.03. The man begins working furiously on his abacus, but Feynman just sits there smiling, and says "12.002" – he knew that there are 1728 cubic inches in a cubic foot.

For years, number theory was thought the "most pure" and least applied branch of mathematics, dealing with 200-digit numbers that can't possibly correspond to counting anything meaningful. But with the advent of Public-Key crypto, suddenly it's one of the most economically and militarily important branches of math.