


Number Theory!


$$p-1 \equiv_p 1$$

$n \mid m$ means that m is an integer multiple of n .

We say that “ n divides m ”.

$$\begin{array}{ll} 2 \mid 4 & 2 \text{ divides } 4 \\ 7 \mid 21 & 7 \text{ divides } 21 \end{array}$$

If $n \mid m$, then m/n has no remainder.

Integer Division

Let a and $n \neq 0$ be integers.


$$\begin{array}{r} a \\ --- \\ n \end{array}$$

$(a \bmod n)$ means


“the remainder when a is divided by n ”

When we divide a by n , get

$$a = q*n + r, 0 \leq r < n$$

We say that $r = (a \bmod n)$
and $q = (a \operatorname{div} n)$

$(a \bmod n)$ means
“the remainder when a is
divided by n ”



Let $0 < a < n$
 $(a \bmod n) = 0$
is equivalent to
 $a \mid n$

The Primes and The Composites

Definition. A natural number n is **prime** if its only factors are 1 and n .

To put it another way: n is **prime** means:
($x \mid n$ implies that $x = 1$ or $x = n$)

Def: A natural number n is **composite** if it is not prime.
(n has some interesting prime factor)

Theorem (Euclid, 300 BC)

Theorem: There are infinitely many primes.

Proof: By Contradiction!

Suppose p_1, \dots, p_k are all the primes.

Let $P = p_1 * \dots * p_k + 1$.

P must be composite. (Why?)

So there is a prime p_i where p_i divides P .

But for every j , if we divide P by p_j we

get: $p_1 \dots p_{j-1} p_{j+1} \dots p_k$ with remainder 1.

So p_i does not divide P ...

CONTRADICTION!

The GCD

$GCD(A,B)$ is the greatest common divisor, the largest number that divides both A and B .

$GCD(A,B) =$ largest n where $n \mid A$ and $n \mid B$.

What is the GCD of 12 and 18?

$$12 = 2^2 * 3 \quad 18 = 2 * 3^2$$

Common factors: 2^1 and 3^1

Answer: 6

How to find $GCD(A,B)$?

Factor the number A into all its prime powers.

Factor the number B into all its prime powers.

Make sets P_A and P_B of the primes dividing A , and all the primes dividing B .

$g := 1$;

For every prime p that is in both P_A and P_B ,

Find the largest a where $p^a \mid A$ and $p^a \mid B$.

$g := g * p^a$;

End for

Return g

Hang on!

This requires factoring A and B .

No one knows a fast way to factor large numbers in general.

EUCLID (300 B.C.) had a much better way to compute GCD!

Ancient Recursion: Euclid's GCD algorithm

```
Euclid(A,B) // requires  $A \geq B \geq 0$   
If  $B=0$  then return  $A$   
else return Euclid(B, A mod B)
```

A small example

```
Euclid(A,B) // requires A ≥ B ≥ 0
If B=0 then return A
else return Euclid(B, A mod B)
```

Note: $GCD(67, 29) = 1$

```
Euclid(67,29)      67 mod 29 = 9
Euclid(29,9)       29 mod 9  = 2
Euclid(9,2)        9 mod 2   = 1
Euclid(2,1)        2 mod 1   = 0
Euclid(1,0) outputs 1
```

But is it correct?

```
Euclid(A,B) // requires A ≥ B ≥ 0
If B=0 then return A
else return Euclid(B, A mod B)
```

Claim: $GCD(A,B) = GCD(B, A \bmod B)$

$d \mid A$ and $d \mid B \Leftrightarrow d \mid (A - kB)$

The set of common divisors of A, B equals the set of common divisors of $B, A - kB$.

Does the algorithm stop?

```
Euclid(A,B) // requires A ≥ B ≥ 0
If B=0 then return A
else return Euclid(B, A mod B)
```

Claim: $A \bmod B < \frac{1}{2} A$

Proof:

If $B > \frac{1}{2} A$ then $A \bmod B = A - B < \frac{1}{2} A$
 If $B < \frac{1}{2} A$ then any $X \bmod B < B < \frac{1}{2} A$
 If $B = \frac{1}{2} A$ then $A \bmod B = 0$

Does the algorithm stop?

```
Euclid(A,B) // requires A ≥ B ≥ 0
If B=0 then return A
else return Euclid(B, A mod B)
```

$GCD(A,B)$ calls $GCD(B, A \bmod B)$

Less than $\frac{1}{2}$ of A

Euclid's GCD Termination

```
Euclid(A,B) // requires A ≥ B ≥ 0
If B=0 then return A
else return Euclid(B, A mod B)
```

$GCD(A,B)$ calls $GCD(B, <\frac{1}{2}A)$

Euclid's GCD Termination

```
Euclid(A,B) // requires A ≥ B ≥ 0
If B=0 then return A
else return Euclid(B, A mod B)
```

$GCD(A,B)$ calls $GCD(B, <\frac{1}{2}A)$

which calls $GCD(<\frac{1}{2}A, B \bmod <\frac{1}{2}A)$

Less than $\frac{1}{2}$ of A

Euclid's GCD Termination

```
Euclid(A,B)    // requires  $A \geq B \geq 0$   
If B=0 then return A  
else return Euclid(B, A mod B)
```

That is:
Every two recursive calls, the input numbers drop by half.

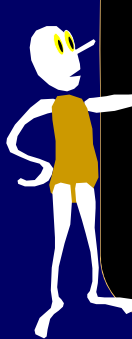
Euclid's GCD Termination

```
Euclid(A,B)    // requires  $A \geq B \geq 0$   
If B=0 then return A  
else return Euclid(B, A mod B)
```

Theorem:


If A and B take n bits to describe, Then Euclid(A,B) will terminate in at most $2n$ recursive calls.

Corollary: GCD is in P




Trick Question:

If A and B are less than n, what is a reasonable upper bound on the number of recursive calls Euclid(A,B) will make?



Answer:

If X and Y are less than n, Euclid(X,Y) will make no more than $2 \log_2 n$ calls.



Modular equivalence of integers a and b:

$$a \equiv b \pmod{n}$$
$$a \equiv_n b$$

"a and b are equivalent modulo n" means that

$$(a \bmod n) = (b \bmod n)$$


\equiv_n is an equivalence relation

In other words,


Reflexive:
 $a \equiv_n a$

Symmetric:
 $(a \equiv_n b) \Rightarrow (b \equiv_n a)$


Transitive:
 $(a \equiv_n b \text{ and } b \equiv_n c) \Rightarrow (a \equiv_n c)$




$a \equiv_n b$ means $(a \bmod n) = (b \bmod n)$
 "a and b are equivalent modulo n"
 \equiv_n partitions the integers into
 n different classes
 We say a and b are in the same
 "congruence class" exactly when $a \equiv_n b$.




The equivalence class $[a]$ is
 the set of all integers that are
 equivalent to a modulo n.
 Let $n = 2$. Then:
 $\{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$
 $[0] = \{\dots, -4, -2, 0, 2, 4, \dots\}$
 $[1] = \{\dots, -3, -1, 1, 3, \dots\}$




The equivalence class $[a]$ is
 the set of all integers that are
 equivalent to a modulo n.
 Let $n = 3$. Then:
 $\{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}$
 $[0] = \{\dots, -6, -3, 0, 3, 6, \dots\}$
 $[1] = \{\dots, -5, -2, 1, 4, 7, \dots\}$
 $[2] = \{\dots, -4, -1, 2, 5, 8, \dots\}$



Equivalence Classes Mod 3:
 $[0] = \{\dots, -6, -3, 0, 3, 6, \dots\}$
 $[1] = \{\dots, -5, -2, 1, 4, 7, \dots\}$
 $[2] = \{\dots, -4, -1, 2, 5, 8, \dots\}$
 $[-6] = \{\dots, -6, -3, 0, 3, 6, \dots\}$
 $[7] = \{\dots, -5, -2, 1, 4, 7, \dots\}$
 $[-1] = \{\dots, -4, -1, 2, 5, 8, \dots\}$




Fundamental Lemma of plus,
 minus, and times modulo n:
 If $(x \equiv_n y)$ and $(a \equiv_n b)$
 Then: $x + a \equiv_n y + b$
 $x - a \equiv_n y - b$
 $x * a \equiv_n y * b$



Fundamental Lemma of plus
 minus, and times modulo n:
 When doing plus, minus, and times
 modulo n, at any time in the
 calculation we can replace a
 number with another number in
 the same equiv. class modulo n


Theorem: $(a \bmod n) = (b \bmod n)$
 $\Leftrightarrow n \mid (a-b)$

Proof: $(a \bmod n) = (b \bmod n)$
 $\Leftrightarrow a \equiv_n b$ ← by definition of \equiv_n
 $\Leftrightarrow (a-b) \equiv_n 0$ ← by Lemma
 $\Leftrightarrow (a-b \bmod n) = 0$ ← by definition of \equiv_n
 $\Leftrightarrow n \mid (a-b)$ ← no remainder!




Please calculate in your head:

$$329 * 666 \bmod 331$$

$$-2 * 4 = -8 = 323$$


A Unique Representation System Modulo n:

We pick exactly one representative from each class. We do all calculations using the representatives.



The integers modulo n:


$$Z_n = \{0, 1, 2, \dots, n-1\}$$

Define a new $+_n$ and $*_n$:

$$a +_n b = (a + b \bmod n)$$

$$a *_n b = (a * b \bmod n)$$

These definitions make sense...




The integers modulo 3

$$Z_3 = \{0, 1, 2\}$$

Two binary operations on Z_3 :

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1




The integers modulo 2

$$Z_2 = \{0, 1\}$$

Two binary operations on Z_2 :

$+_2$	0	1
0	0	1
1	1	0

$*_2$	0	1
0	0	0
1	0	1




The Boolean interpretation of $Z_2 = \{0, 1\}$

0 means FALSE 1 means TRUE

$+_2$ XOR	0	1
0	0	1
1	1	0


$*_2$ AND	0	1
0	0	0
1	0	1



The integers modulo 4
 $Z_4 = \{0, 1, 2, 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2


*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1



The integers modulo 5
 $Z_5 = \{0, 1, 2, 3, 4, 5\}$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1




Suppose p is a prime
Fundamental Lemma of division modulo p

If $0 < c < p$ and $ca \equiv_p cb$,
then $a \equiv_p b$


$Z_p^* = \{1, \dots, p-1\}$

Over Z_p^* , we can both
multiply and divide!



$Z_5^* = \{1, 2, 3, 4\}$


$*_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1



$Z_n = \{0, 1, 2, \dots, n-1\}$
When p is prime: $Z_p^* = \{1, 2, \dots, p-1\}$


$a +_n b = (a+b \text{ mod } n)$ $a *_n b = (a*b \text{ mod } n)$

Theorem: When p is prime,
we can add, subtract, multiply
and divide efficiently in Z_p !
A little number universe,
all to itself...




Fermat's Little Theorem
 If p is prime, and a is in Z_p^*
 then $a^{p-1} \equiv_p 1$

Proof: If we prove $a^p \equiv_p a$,
 then we can divide both sides by p !




Fermat's Little Theorem
 If p is prime, and a is in Z_p^*
 then $a^{p-1} \equiv_p 1$

Proof: How can we prove $a^p \equiv_p a$?
 We need to prove that $p \mid (a^p - a)$.
 If we prove $(a^p - a)/p$ is an integer
 then we are done!



Fermat's Little Theorem
 If p is prime, and a is in Z_p^*
 then $a^{p-1} \equiv_p 1$


Proof: How can we prove that
 $(a^p - a)/p$ is an integer?
 We will invent up some concrete
 objects and argue that the total
 number of them is $(a^p - a)/p$



Fermat's Little Theorem
 If p is prime, and a is in Z_p^*
 then $a^{p-1} \equiv_p 1$

Want: $(a^p - a)/p$ is an integer


Proof: Counting bracelets. Suppose
 we have a possible bead colors.
 A bracelet of beads is colorful if
 not all beads have the same color.
 Let N be the number of colorful
 bracelets with exactly p beads.



Fermat's Little Theorem
 If p is prime, and a is in Z_p^*
 then $a^{p-1} \equiv_p 1$

Want: $(a^p - a)/p$ is an integer

Claim: $N = (a^p - a)/p$
 There are a^p different ways to line
 up p beads (with " a " possible colors)
 on a string. Only " a " of these
 strings have all p beads with the
 same color. Subtract those out.



Claim: $N = (a^p - a)/p$

So there are $a^p - a$ colorful strings.
 Suppose we connect the two ends
 of each colorful string together to
 form a bracelet. For every string s ,
 there are exactly $p-1$ other strings
 that make identical bracelets to s .
 So the total number of distinct
 colorful bracelets is $N = (a^p - a)/p$