Number Theory

Last lecture:

GCD and Linear Combinations

Today:

Prime numbers and factorization

Modular Arithmetic

Perfect Numbers

Perfect Numbers (300 BC): N is perfect if its divisors sum to N.

Examples:

6 = 1 + 2 + 3

28 = 1 + 2 + 4 + 7 + 14

496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248

8128

33550336

Open Questions: Are there infinitely many perfect numbers?

Is there even one odd perfect number?

(It will have to be bigger than 10^{1500}!!!

What we know about Perfect Numbers

Euclid (300 BC): If $2^p - 1$ is prime then $2^{p-1}(2^p - 1)$ is perfect

Conjecture (100 AD): Every even perfect number is of the form $2^{p-1}(2^p - 1)$

where $2^p - 1$ is prime.

Conjecture proved by Euler in the 18^{th} century.

As of January 2018, 50 perfect numbers were known – largest was

$$2^{77232916}(2^{77232917} - 1)$$

As of today, the 51^{st} perfect number $2^{82589933}(2^{82589934} - 1)$

The Fundamental Theorem of Arithmetic

Theorem: Every number greater than 1 is uniquely expressed as a product of primes.

The natural number $p > 1$ is prime if $\forall n < p\ \gcd(n, p) = 1$

Lemma 1: If p is prime and $p|ab$ then $p|a \vee p|b$

Proof: $\gcd(p, a) = 1\ or\ p$.

$\gcd(p, a) = p \Rightarrow p|a$

$\gcd(p, a) = 1 \Rightarrow p|b$ (GCD lemma, part d)

Lemma 2: Every number greater than 1 can be expressed as a product of primes.

Proof: Use the well-ordering principle (or strong induction).

The Fundamental Theorem of Arithmetic

Theorem: Every number greater than 1 is uniquely expressed as a product of primes.

Proof of Uniqueness: Let $N = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ be the smallest number expressible as the product of primes in two different ways.

$p_1 | N \Rightarrow p_1 | q_i$, for some $i \le l$. (by Lemma 1)

But this means $p_1 = q_i$.

So $N' = p_2 \cdots p_k = q_1 \cdot\cdot q_{i-1} q_{i+1} \cdot\cdot q_l$ is expressible as the product of primes in two different ways.

But $N' < N$, contradicting our assumption.

Therefore, the prime factorization of every number is unique.

Prime Numbers

A natural number $p > 1$ is prime if $\forall n < p \;\; \gcd(n, p) = 1$

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, …

How many numbers are prime?

Theorem: There are infinitely many primes.

Proof: Assume otherwise and let $p_1 < p_2 < \cdots < p_k$ be the finite set of primes.

Consider the number $P = 1 + p_1 \cdot p_2 \cdots p_k$

Since $1 = P - p_i(p_1 \ldots p_{i-1} p_{i+1} \ldots p_k)$, $\gcd(p_i, P) = 1$

Therefore, $\forall i \leq k \colon p_i \nmid P$

So P must be prime.

But $P > p_k$, the largest prime, which contradicts our assumption.

Therefore, the set of primes is infinite.

Modular Arithmetic

The study of remainders, sometimes also called “clock arithmetic”

Example: hours of the day, days of the week, months of the year, …

Let $m \in \mathbb{N}, m > 0$.

What are all possible remainders when an integer is divided by m?

By the division theorem, $\forall a \in \mathbb{Z},\ a = qm + r,\ 0 \leq r < m$

The set of all possible remainders is $\mathbb{Z}_m = \{0,1, \dots, m-1\}$

We commonly say that $r = a\ mod\ m$

I prefer to say $r = rem(a, m)$ to avoid confusion

Congruence modulo m

Definition: Integers a, b are ***congruent modulo m*** if and only if $m|a - b$

Notation: $a \equiv b\ (mod\ m)$ is shorthand for "a, b are *congruent modulo m*"

Examples:

$25\ \equiv 4\ (mod\ 7)$ because $7|(25 - 4)$

$25\ \not\equiv 4\ (mod\ 11)$ because 11 does not divide 21.

"congruence mod m" is a relation – (a different relation for every choice of m)

"congruence" by itself is not a relation.

The notation $a \equiv_m b$ would have been better, but we're stuck with tradition.

A Basic Theorem

Theorem: $a \equiv b \ (mod\ m) \Leftrightarrow rem(a, m) = rem(b, m)$

Proof: Let $a = mq_1 + r_1$, $b = mq_2 + r_2$,

so that $a - b = m(q_1 - q_2) + (r_1 - r_2)$, where $-m < r_1 - r_2 < m$

$\Rightarrow$

$a \equiv b \ (mod\ m)$

$\Rightarrow m \mid (a - b)$, by definition

$\Rightarrow m \mid m(q_1 - q_2) + (r_1 - r_2)$

$\Rightarrow m \mid r_1 - r_2$

$\Rightarrow r_1 - r_2 = 0$

$\Rightarrow r_1 = r_2$

$\Leftarrow$

$a - b = m(q_1 - q_2) + (r_1 - r_2)$

$r_1 = r_2$

$\Rightarrow \ a - b = m(q_1 - q_2)$

$\Rightarrow \ m \mid a - b$

$\Rightarrow \ a \equiv b \ (mod\ m)$

Congruence mod m is an equivalence relation

Lemma: The following properties hold for every $m \in \mathbb{N}^+$

1. $a \equiv a \ (mod\ m)$ Reflexive
2. $a \equiv b \ (mod\ m) \Longrightarrow b \equiv a \ (mod\ m)$ Commutative
3. $a \equiv b \ (mod\ m) \ \wedge \ b \equiv c \ (mod\ m) \ \Longrightarrow \ a \equiv c \ (mod\ m)$ Transitive

Example: Equivalence classes modulo 5

$\mathbb{Z} \rightarrow$	0,5,10,15,…	1,6,11,16,…	2,7,12,17,…	3,8,13,18,…	4,9,14,19,…
class property	rem 0	rem 1	rem 2	rem 3	rem 4
Representative	**0**	**1**	**2**	**3**	**4**

Modular Arithmetic

Lemma:

1. $a \equiv b \ (mod\ m) \implies a + c \equiv b + c \ (mod\ m)$ Add common term to both sides.
2. $a \equiv b \ (mod\ m) \implies a \cdot c \equiv b \cdot c \ (mod\ m)$ Multiply by common term on both sides.
3. $a \equiv b \ (mod\ m) \ \wedge \ c \equiv d \ (mod\ m) \implies a + c \equiv b + d \ (mod\ m)$ Add equal numbers.
4. $a \equiv b \ (mod\ m) \ \wedge \ c \equiv d \ (mod\ m) \implies a \cdot c \equiv b \cdot d \ (mod\ m)$ Multiply equal numbers.

Proof of 3:

$$a \equiv b \ (mod\ m) \Rightarrow a + c \equiv b + c \ (mod\ m) \text{ (from 1)}$$

$$c \equiv d \ (mod\ m) \Rightarrow b + c \equiv b + d \ (mod\ m) \text{ (from 1)}$$

$$\Rightarrow \quad a + c \equiv b + d \ (mod\ m)$$

So far it looks just like normal arithmetic …..

Where things go haywire

If $a \cdot c \equiv b \cdot c\ (mod\ m)$ does it mean that $a \equiv b\ (mod\ m)$?

If $c = 0$ then this is not true!

But what if $c \neq 0$?

Example: $4 \cdot 3 \equiv 9 \cdot 3\ (mod\ 5) \quad and \ \ 4 \equiv 9\ (mod\ 5)$

Counterexample: $3 \cdot 2 \equiv 1 \cdot 2\ (mod\ 4)$ but $3 \not\equiv 1\ (mod\ 4)$

How do we know when it's safe to cancel common factors?

GCD to the rescue!

Theorem: If $a \cdot c \equiv b \cdot c \ (mod\ m)$ and $\gcd(c, m) = 1$ then $a \equiv b \ (mod\ m)$.

It is safe to cancel a common factor that is relatively prime to the modulus.

Proof: $a \cdot c \equiv b \cdot c \ (mod\ m)$

$$\Rightarrow m \mid (a - b)c$$

Since $\gcd(c, m) = 1$, it follows from the GCD lemma (part d) that

$$m \mid (a - b)$$

But this implies that $a \equiv b \ (mod\ m)$.

Friday the 13^{th}

Does every year have a month in which the 13^{th} day is Friday?