Number Theory

Last lecture:

The division theorem

Today:

Linear Combinations and GCD

Other unsolved problems

Twin primes conjecture (1862): There are infinitely many pairs of primes that differ by 2.

2013: There are infinitely many pairs of primes that differ by $N, N < 70{,}000{,}000$

2014: $N < 246$

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

Are there infinitely many perfect numbers?

Greatest Common Divisor

The gcd of integers a, b, denoted $\gcd(a, b)$ is the largest integer that divides both a and b.

$$\gcd(42, 48) = 6$$
$$\gcd(15, 40) = 5$$
$$\gcd(162, 90) = 18$$

One way to compute the gcd, factor each number into primes, and extract the common part.

$$\gcd(81169704, 1914823911)$$
$$\begin{aligned} &= \gcd(2^3 3^2 7^1 11^5, 3^1 7^4 11^2 13^3) \\ &= 3^1 7^1 11^2 \\ &= 2541 \end{aligned}$$

But factoring is hard, and we don't have any efficient factoring algorithms!

Linear Combinations

The expression $sa + tb$ is a linear combination of two integers a, b.

The set $\{sa + tb : s, t \in \mathbb{Z}\}$ is the set of all integer linear combinations of a, b.

Example: $a = 12, b = 30$

The set of all integer linear combinations is $\{12s + 30t : s, t \in \mathbb{Z}\}$

$\boldsymbol{s}$	$\boldsymbol{t}$	$\mathbf{12}\boldsymbol{s} + \mathbf{30}\boldsymbol{t}$
-3	1	-6
-3	2	24
-2	0	-24
-2	1	6
-1	1	18
0	0	0

What is the smallest possible positive value of $12s + 30t$?

GCDs and Linear Combinations

GCD Theorem. The smallest positive linear combination m of two integers a, b (at least one of which is non-zero) equals $g = \gcd(a, b)$.

Consequently, the smallest positive linear combination of 12, 30 is $\gcd(12,30) = 6$

We'll prove the theorem in three parts:

i. Prove that the smallest positive linear combination exists for all pairs a, b

ii. Prove that $g \leq m$ (m is the smallest positive linear combination)

iii. Prove that $g \geq m$.

Proof of the GCD Theorem…part i

Let a, b be any pair of integers, at least one non-zero.

Consider the linear combination $sa + tb$:

By choosing s to have the same sign as a, and t to have the same sign as b,

we can construct infinitely many positive linear combinations

By the well-ordering principle, there is a smallest positive linear combination of a, b.

Proof of the GCD Theorem…part ii

Proof that $g \leq m$:

Since $g \mid a \;\;\wedge\;\; g \mid b,$ it follows from the divisibility lemma (part c) that

$$\forall s, t \in \mathbb{Z} \quad g \mid sa + tb$$

In particular, $g \mid m$

Since $m > 0$ it follows that $g \leq m$.

Proof of the GCD Theorem…part iii

Proof that $g \geq m$.

Since m is a linear combination, we can express $m = sa + tb$

By the division theorem, $a = qm + r, \quad 0 \leq r < m$

Substituting for m, we get $a = q(sa + tb) + r$

Rearranging terms, we get $r = (1 - qs)a + (-qt)b$

This means that r is a linear combination of a, b and is smaller than m.

Since m is the smallest positive linear combination, it follows that $r = 0$.

Therefore, $m \mid a$.

Repeating the argument with b, we have that $m \mid b$.

Since m is a common divisor of a, b it follows that $m \leq g$ (the greatest common divisor of a, b)

GCD and Linear Combinations

Lemma. An integer is a linear combination of a, b $if\ and\ only\ if$ it is a multiple of $\gcd(a, b)$.

Proof:

(i) $g \mid a \wedge g \mid b \Rightarrow g \mid sa + tb$ (every l.c. is a multiple of the gcd)

(ii) $N = kg \Rightarrow N = k(sa + tb)$ (because g is a l.c. of a, b)

$\Rightarrow N = (ks)a + (kt)b$

So N is a l.c. of a, b.

$\boldsymbol{s}$	$\boldsymbol{t}$	$\mathbf{12}\boldsymbol{s} + \mathbf{30}\boldsymbol{t}$
-3	1	-6
-3	2	24
-2	0	-24
-2	1	6
-1	1	18
0	0	0

The GCD Lemma

GCD Lemma. The following statements are true.

a. $\forall c \in \mathbb{Z}\colon\ (c|a \ \wedge\ c|b) \implies c|\gcd(a,b)$

b. $\forall k > 0\colon\ \gcd(ka,kb) = k \cdot \gcd(a,b)$

c. $(\gcd(a,b) = 1 \ \wedge\ \gcd(a,c) = 1\,) \implies \gcd(a,bc) = 1$

d. $(a|bc \ \wedge\ \gcd(a,b) = 1) \implies a|c$

e. $\gcd(a,b) = \gcd(b, rem(a,b))$

where $rem(a,b)$ is the remainder on dividing a by b.

Euclid's Algorithm for GCD

$\gcd(a, b) = \gcd(b, rem(a, b))$, where $rem(a, b)$ is the remainder on dividing a by b.

What is $\gcd(1147{,}899)$?

$$
\begin{aligned}
1147 &= 899 + 248 \\
899 &= 3 \cdot 248 + 155 \\
248 &= 155 + 93 \\
155 &= 93 + 62 \\
93 &= 62 + 31 \\
62 &= 2 \cdot 31 + 0
\end{aligned}
$$

$$
\begin{aligned}
\gcd(1147, 899) &= \gcd(899, 248) \\
&= \gcd(248, 155) \\
&= \gcd(155, 93) \\
&= \gcd(93, 62) \\
&= \gcd(62, 31) \\
&= \gcd(31, 0) \\
&= 31
\end{aligned}
$$

Theorem: The number of steps is no greater $2\log_2 a$ (twice the number of bits of a).

GCDs as linear combinations

Since $\gcd(1147, 899) = 31$ we know that 31 is a linear combination of 1147 and 899.

In other words, there exist integers s, t such that $1147s + 899t = 31$.

But what are s, t? How do we compute them?

The "Pulverizer"

$$\begin{aligned}\gcd(1147, 899) &= \gcd(899, 248)\\ &= \gcd(248, 155)\\ &= \gcd(155, 93)\\ &= \gcd(93, 62)\\ &= \gcd(62, 31)\\ &= \gcd(31, 0)\\ &= 31\end{aligned}$$

$$\begin{aligned}1147 &= 899 + 248\\ 899 &= 3 \cdot 248 + 155\\ 248 &= 155 + 93\\ 155 &= 93 + 62\\ 93 &= 62 + 31\\ 62 &= 2 \cdot 31 + 0\end{aligned}$$

$$\begin{aligned}31 &= 93 - 62\\ &= 93 - (155 - 93)\\ &= 2 \cdot 93 - 155\\ &= 2 \cdot (248 - 155) - 155\\ &= 2 \cdot 248 - 3 \cdot 155\\ &= 2 \cdot 248 - 3 \cdot (899 - 3 \cdot 248)\\ &= 11 \cdot 248 - 3 \cdot 899\\ &= 11 \cdot (1147 - 899) - 3 \cdot 899\\ &= 11 \cdot 1147 - 14 \cdot 899\end{aligned}$$

Also known as the Extended Euclidean algorithm

So $s = 11, \quad t = -14$

Quick Summary

Euclid’s algorithm to compute GCD

Pulverizer to express the GCD as a linear combination

We will use both frequently.

Applications?

DIE HARD 3: With a Vengeance

You have a 3-gallon jug and a 5-gallon jug, and unlimited water supply.

Can you measure exactly 4 gallons?

In one step you may:

fill a jug with water

pour water from one jug into another

empty a jug, throwing away the water

1. Fill the 3-gallon jug (3, 0)
2. Empty the 3-g jug into the 5-g jug (0, 3)
3. Fill the 3-g jug (3, 3)
4. Pour from the 3-g jug until the 5-g jug is full (1, 5)
5. Empty the 5-g jug (1, 0)
6. Empty the 3-g jug into the 5-g jug (0, 1)
7. Fill the 3-g jug (3, 1)
8. Empty the 3-g jug into the 5-g jug (0, 4) !!!

Can you measure 3 gallons using 21- and 26-gallon jugs? 4 gallons using 3- and 6-gallon jugs?

How much water in a jug?

With jugs of capacities a, b every measurable amount is a linear combination of a, b!

Claim: At the end of a round, the amount in the small jug is 0, and in the larger jug a l.c. of a, b.

Proof: By induction on the number n of rounds.

Base Case: $n = 0$. Both jugs are empty, and $0 = 0 \cdot a + 0 \cdot b$

I.H.: After k rounds, the amount in the small jug is 0, and the larger jug contains a l.c. of a, b.

I.S.: At the end of round k, the amounts are $0, j$ – both are l.c. of a, b.

During the $(k+1)st$ round:

- Fill the small jug $(0, j) \to (a, j)$
- Pour from the small jug into the larger jug, empty the large jug if it becomes full.
  - The larger jug accommodates all the water from the smaller jug: $(a, j) \to (0, a + j)$
  - The larger jug becomes full before the smaller one is emptied: $(a, j) \to (a + j - b, b) \to (0, a + j - b)$

At the end of round $k + 1$: $(0, a + j)\ or\ (0, a + j - b)$. In both cases, the small jug contains – and the larger jug contains a linear combinations of a, b.

GCD strikes!

What about measuring 4 gallons using 3- and 6-gallon jugs?

$\gcd(3,6) = 3$. But 4 is NOT a multiple of the gcd.

So, 4 cannot be measured with these jugs!

What about measuring 3 gallons using 21- and 26-gallon jugs?

$\gcd(21,26) = 1$. So, 3 is a multiple of the gcd.

But can we do it?