Number Theory

"G-d created the integers,
all else is the work of man", Kronecker

Number theory is the study of integers, more specifically divisibility properties of integers.

$m \mid n$ denotes that m divides n, or
$n = km$ for some integer k.

$m \nmid n$ denotes that m does not divide n

This is equivalent to saying n is a multiple of m, and this gives two quantities

$$\gcd(m,n) = \max\{k \mid k \mid m \text{ and } k \mid n\}$$

greatest common divisor is the largest integer which divides both m & n

$$\operatorname{lcm}(m,n) = \min\{k \mid k>0,\ m \mid k \text{ and } n \mid k\}$$

least common multiple is the smallest integer which is a multiple of m & n.

$\gcd(18,12) = 6$ $\quad \operatorname{lcm}(18,12) = 36$

Euclid's Algorithm for GCD

The world's oldest interesting algorithm is Euclid's for computing the GCD

$$\gcd(0, N) = N$$

$$\gcd(M, N) = \gcd(N \bmod M, M), \text{ for } M > 0$$

$$\begin{aligned}
\gcd(963, 657) &= \gcd(657, 963-657) \\
&= \gcd(657, 306) \\
&= \gcd(306, 657-2\cdot 306) \\
&= \gcd(306, 45) \\
&= \gcd(45, 36) \\
&= \gcd(36, 9) \\
&= \gcd(9, 0) = \underline{9}
\end{aligned}$$

why? Suppose $d \mid N$ & $d \mid M$

$$N \bmod M = N - \lfloor N/M \rfloor M$$

$$= d\left(\frac{N}{d} - \frac{M}{d}\lfloor N/M \rfloor\right)$$

Thus no divisor is lost in taking the remainders, and the gcd is preserved!

Note that we can prove that a number is in fact the gcd iff we can find m', n' such that

$$m'm + n'n = \gcd(m,n)$$

Why? If $d \mid m$ and $d \mid n$, then $d \mid (m'm + n'n)$ if m', n' are integers. Thus $d = \gcd(m,n)$ is the greatest common divisor of m & n!

We can compute an appropriate m', n' using Euclid's algorithm:

Basis case: $\gcd(0,n) = n$

$$\underset{m'}{0} \cdot 0 + \underset{n'}{1} \cdot n = n$$

General case: $\gcd(m,n) = \gcd(n \bmod m, m)$

$$r = n - m\lfloor n/m \rfloor \quad = \gcd(r,m)$$

therefore, $\bar{r}\, r + \bar{m}\, m = \gcd(r,m)$ (by induction)

$$\bar{r}(n - m\lfloor n/m \rfloor) + \bar{m}\, m = \gcd(m,n)$$

$$\underset{n'}{\bar{r}}\, n + (\underbrace{\bar{m} - \bar{r}\lfloor n/m \rfloor}_{m'})\, m = \gcd(m,n)$$

Example: gcd(963, 657)

From previous example $= \gcd(657, 306)$

$= \gcd(306, 45)$

$= \gcd(45, 36)$

$= \gcd(36, 9)$

$= \gcd(9, 0)$

N'		M'		
$9 \cdot 1$	$+$	$0 \cdot 0$	$=$	9
$36 \cdot 0$	$+$	$9(1 - 0 \cdot \lfloor \frac{36}{9} \rfloor)$	$=$	9
$45 \cdot 1$	$+$	$36(0 - 1 \lfloor \frac{45}{36} \rfloor)$	$=$	9
$306 \cdot -1$	$+$	$45(1 - -1 \lfloor \frac{306}{45} \rfloor)$	$=$	9
$657 \cdot 7$	$+$	$306(-1 - 7 \lfloor \frac{657}{306} \rfloor)$	$=$	9
$963 \cdot -15$	$+$	$657(7 - -15 \lfloor \frac{963}{657} \rfloor)$	$=$	9

$963 \cdot -15 + 657 \cdot 22 = 9$

$m' = \bar{m} - \lfloor N/m \rfloor \bar{N}$

Prime Numbers

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

A positive integer is prime if it has exactly two divisors. 1 is not prime as a general convenience.

Any integer which is not prime is <u>composite</u>.

Any composite can be written as the product of primes:

$$N = p_1 \cdots p_n = \prod_{i=1} p_i$$

The Fundemental Theorem of Arithmetic

states that there is a unique factorization of N into primes.

Proof by contradiction:

Let $N = p_1 p_2 \cdots p_M = 2 \cdot 7_2 \cdots 7_k$ be the smallest N with two distinct prime factorizations.

Thus $p_1 < q_1$ WLOG.

Since $p_1 \perp q_1$, $p_1 a + q_1 b = 1$

multiply both sides by $q_2 \cdots q_k$

$$a \underbrace{p_1 q_2 \cdots q_k} + bN = \underbrace{q_2 \cdots q_k}$$

divisible by p_1 $\therefore$ must be divisible by p_1, but can't be since $q_2 \cdots q_k$ has a unique prime factorization without p_1

This gives us a unique way to represent integers by the exponents of their prime factorizations

$$N = \prod_p p^{N_p} \qquad N \Rightarrow \{N_2, N_3, N_5, \ldots\}$$

$$12 = \{2, 1, 0, 0 \ldots\}$$

$$18 = \{1, 2, \ldots\}$$

Thus adding these exponents "multiplies" the numbers.
Note that no shifting is necessary to rebalance.

The greatest common divisor results from taking the pairwise MIN of the two sets of exponents.

The least common multiple results from the pairwise MAX of the two sets of exponents.

Such number theoretic features suggest alternate number systems which occasionally appear useful for computation. But how do you add two numbers with this representation?

The Density of Primes

Euclid's proof shows there are an infinite number of primes, but doesn't really tell how many there are

The n^{th} largest prime $p_n \sim n \ln n$

The number of primes less than x,

$$\pi(x) \sim x/\ln x$$

Thus there are a lot of them out there, which causes some counter-intuitive results:

Goldbach's conjecture states that every even integer is the sum of two primes

$$14 = 3 + 11 \qquad 16 = 11 + 5 = 3 + 13$$

It is a famous open problem to prove Goldbach's conjecture. The reason it is hard is the same reason it is (probably) true - that there are so many primes that the expected number of representations increases with n.

Factorial Factors

The factorial function is kind of an "anti-prime" function, since it creates highly composite numbers.

$$0! = 1$$

$$N! = N\,(N-1)! = \prod_{k=1}^{N} k$$

This recurrence is defined only for integers, but the Gamma function $\Gamma(N)$ generalizes it to reals with the property that

$$\Gamma(N) = (N-1)\,\Gamma(N-1), \quad N \geq 1$$

so $N! = \Gamma(N+1)$

How big is $N!$?

$$\left(\frac{N}{k}\right)^{N-\frac{N}{k}} \leq N! \leq N^N$$

so it grows something like $O(N^N)$, consistant with Stirling's approximation: $N! \simeq \sqrt{2\pi N}\left(\frac{N}{e}\right)^N$

Stirling's approximation is a slight upper bound on $N!$

Permutations and Combinations

The most elementary counting problem is the number of permutations on N elements:

$$N \quad (N-1) \quad (N-2) \quad \cdots \quad 1 \quad = N!$$

choices for 1st item; # choices for 2nd item; # choices for 3rd item; # choices for N^{th} item

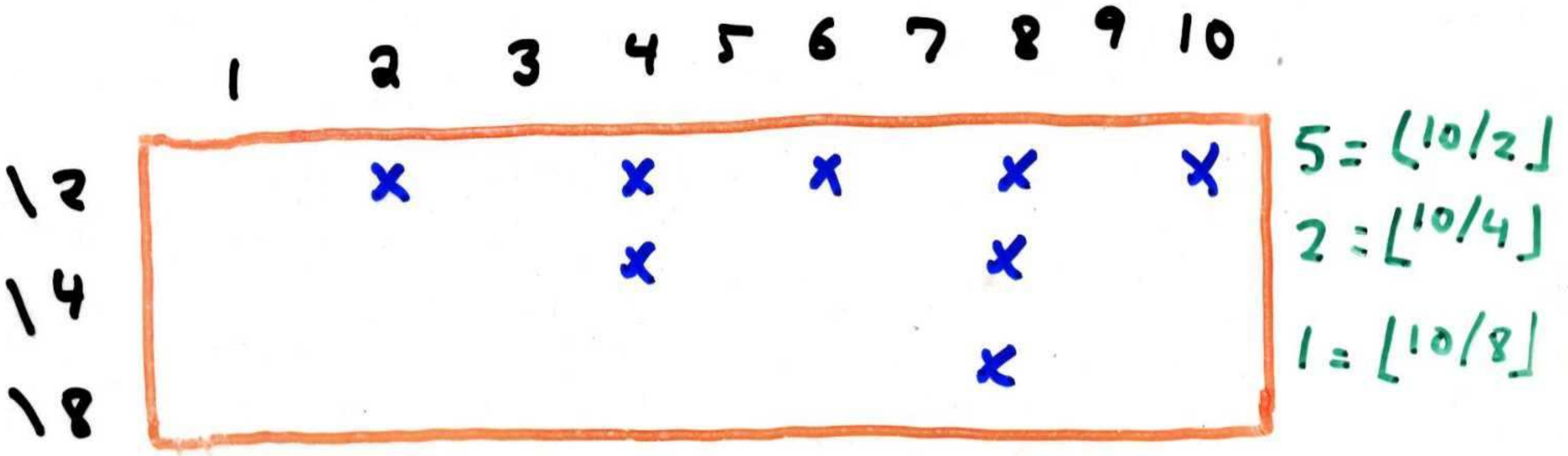
Second most elementary is the number of arrangements of k out of N elements

$$N\,(N-1)\,\ldots\,(N-k+1) = \frac{N!}{(N-k)!}$$

Third most elementary is the number of ways to pick k out of N elements, where order doesn't matter. Since we want only one of $k!$ permutations of k items, $\dfrac{N(N-1)\cdots(N-k+1)}{k\cdot(k-1)\cdots 1} = \dfrac{N!}{k!(N-k)!} = \binom{N}{k}$

But why is $\binom{N}{k}$ always an integer?

What is $\epsilon_p(N!)$, the exponent of prime factor p in N!?



$$\epsilon_p(N!) = \sum_{k \geq 1} \lfloor N/p^k \rfloor$$

For $\binom{N+M}{N}$ to be an integer, for any p,

$$\sum_{k \geq 1} \lfloor (M+N)/p^k \rfloor \overset{\text{must be}}{\geq} \sum_{k \geq 1} \lfloor M/p^k \rfloor + \sum_{k \geq 1} \lfloor N/p^k \rfloor$$

but $\lfloor x+y \rfloor = \lfloor \lfloor x \rfloor + \{x\} + \lfloor y \rfloor + \{y\} \rfloor$

$$= \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \{x\} + \{y\} \rfloor$$

$$\geq \lfloor x \rfloor + \lfloor y \rfloor$$

Since for each k the inequality holds, it holds over the sum. ∎

We can use this formula to get a lower bound on $\pi(x)$

$$\epsilon_p(N!) = \sum_{k\geq 1} \lfloor N/p^k \rfloor \leq \sum_{k\geq 1} N/p^k$$

$$= \frac{N}{p}\left(1 + \frac{1}{p} + \left(\frac{1}{p}\right)^2 + \cdots\right) = \frac{N}{p}\left(\frac{1}{1-\frac{1}{p}}\right)$$

$$= \frac{N}{p}\left(\frac{p}{p-1}\right) = \frac{N}{p-1}$$

Thus each factors "contribution" to $N!$, $\prod_p p^{\epsilon_p(N!)} = N!$

$$p^{\epsilon_p(N!)} \leq p^{N/(p-1)}$$

Since any prime $p > 2$, $2^p \geq 2p \rightarrow p \leq 2^{p-1}$

giving a loose bound on p, so

$$p^{\epsilon_p(N!)} \leq p^{N/(p-1)} \leq \left(2^{p-1}\right)^{N/(p-1)} = 2^N$$

Thus any prime contributes at most 2^N to $N!$

//