COT 3100 2/16/23

(1) N.T. Notes updated (redownload)

(2) Exam, Quiz, Attendance (ree) - update
- Calc Grade (Webcourses is wrong!)
- Relative Where You Stand

Finish up Num Theory

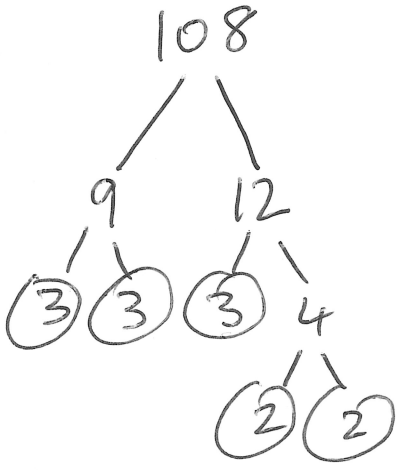
Fun Problems!

Fundamental Thm of Arithmetic

Each pos integer has a unique prime factorization.

p is prime iff $p \geq 2$ and its only divisors are 1 and p.
$p \in \mathbb{Z}$

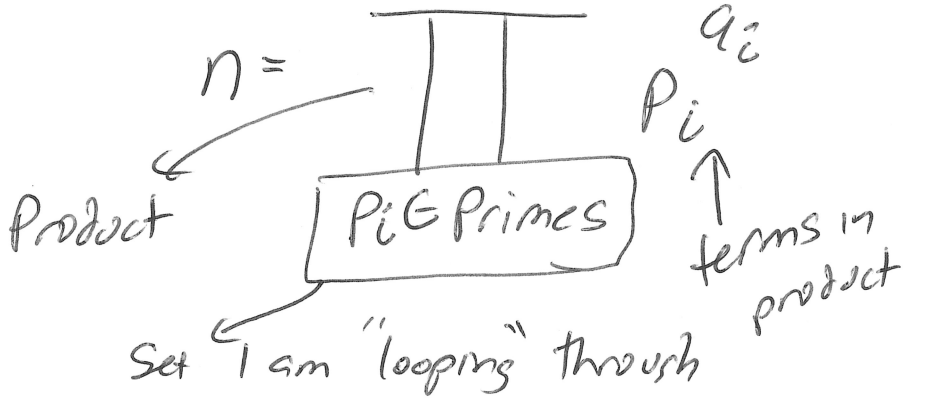
Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...



primes are the building blocks of the integer world much like atoms are the building blocks of molecules, etc.

$= 2^2 \times 3^3$

Formally, all positive integers, n, have a unique representation in the form



, q_i's are non-negative ints

$2^2 3^3 \leftrightarrow [2,3,0,0,\dots]$

$2 \cdot 3 \cdot 7^3 \leftrightarrow [1,1,0,3,0,\dots]$

$78 = 2 \times 3 \times 13 \leftrightarrow [1,1,0,0,0,1,0,\dots]$

Sketch of Proof

Pf by contradiction, assume that n is the smallest int with 2 different valid prime factorizations

$$n = \prod_{p_i \in \text{Primes}} p_i^{q_i} = \prod_{p_i \in \text{Primes}} p_i^{b_i}$$

find smallest $p_k \mid n$ $\quad \frac{\quad}{p_k} \quad \frac{\quad}{p_k} \quad \frac{\quad}{p_k}$

$\gcd(p,q) = 1$ if $p \neq q$ $\quad p, q \in$ Primes

$$p_1^{q_1} p_2^{q_2} \cdots p_k^{q_k - 1} \cdots = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k - 1} \cdots$$

How to prime factorize =
trial division (try 2, 3, 5, 7, ...)

Proof of Infinite # of Primes

Assume the opposite, that there are a finite # of primes. Let these be $p_1, p_2, p_3, \ldots, p_n$.

Consider integer $p_1 \times p_2 \times p_3 \cdots \times p_n + 1$

$$X = \left(\prod_{i=1}^{n} p_i \right) + 1$$

not equal to p_i for any $i \in [1, n]$
$p_i \nmid X$. (remainder = 1 for each division)

X must have a prime factorization, and none of its prime divisors are on the list, thus we get a contradiction about the completeness of the list.

Prime Number Thm # primes from 1 to $n \sim \frac{n}{\ln n}$.

Twin Primes 11, 13 Infinite # of twins? Unknown

Fermat Primes, Mersenne Primes

Least Common Multiple (a, b)

Smallest, pos. integer d such that $a \mid d \wedge b \mid d$

$$a = \prod_{p_i \in Primes} p_i^{a_i}, \quad b = \prod_{p_i \in Primes} p_i^{b_i}$$

$$LCM(a,b) = \prod_{p_i \in Primes} p_i^{\max(a_i, b_i)}$$

$a = 2^3 \times 3^2 \times 5 \times 11^6$

$b = 2^2 \times 3^6 \times 7 \times 11^4$

$LCM(a,b) = 2^3 \times 3^6 \times 5^1 \times 7^1 \times 11^6$

→ a and b guaranteed to divide into this.

each term in LCM divides into a or b.

$$GCD(a,b) = \prod_{p_i \in Primes} p_i^{\min(a_i, b_i)}$$

$gcd(a,b) = 2^2 \times 3^2 \times 11^4$

$$\underline{LCM(a,b) \times GCD(a,b)} = \left(\prod_{p_i \in Primes} p_i^{\max(a_i,b_i)}\right)\left(\prod_{p_i \in Primes} p_i^{\min(a_i,b_i)}\right)$$

$$= \prod_{p_i \in Primes} p_i^{\max(a_i,b_i)} \times p_i^{\min(a_i,b_i)}$$

$$= \prod_{p_i \in Primes} p_i^{\max(a_i,b_i)+\min(a_i,b_i)}$$

$$= \prod_{p_i \in Primes} p_i^{a_i+b_i}$$

$$= \left(\prod_{p_i \in Primes} p_i^{a_i}\right)\left(\prod_{p_i \in Primes} p_i^{b_i}\right)$$

$$= a \times b$$

$$LCM(a,b) = \frac{a \times b}{GCD(a,b)}$$

} allows for efficient computation of LCM

Number of Divisors of an Int

$$n = \prod_{p_i \in \text{Primes}} p_i^{a_i}$$

$n = 2^3 \times 3^2 = 72$

$d = 2^a \times 3^b$, $0 \le a \le 3$ (4)
$0 \le b \le 2$ (3)

any choice a paired w/ any choice b $\Rightarrow$ $4 \times 3 = 12$ divisors

	3^0	3^1	3^2
2^0	1	3	9
2^1	2	6	18
2^2	4	12	36
2^3	8	24	72

$$\tau(n) = \prod_{p_i \in \text{Primes}} (a_i + 1)$$

$184 = 4 \times 46 = 8 \times 23 = 2^3 \times 23^1$

divisors $= (3+1)(1+1) = 8$

72

1 × 72
2 × 36
3 × 24
4 × 18
6 × 12
8 × 9

pairs d, n/d

36

1 × 36
2 × 18
3 × 12
4 × 9
* 6 × 6

→ only way to have odd # of divisors is if

$d = \frac{n}{d} \rightarrow n = d^2$

n is a perfect square

Iff n is a perfect square, does n have an odd # of divisors.

If all $a_i + 1 \in$ Odd, then $a_i \in$ Even $\rightarrow n$ is a perfect square.

If a number, n, is composite, it must have at least 1 divisor, d, $1 < d \leq \sqrt{n}$.

Pf: Assume opposite $n = ab$ w/ $a > \sqrt{n}, b > \sqrt{n}$

$$> \sqrt{n}\sqrt{n}$$
$$= n$$

$n > n$ is a contradiction. Our assumption that all divisors > 1 were $> \sqrt{n}$ is wrong.

Determining Primality (of n)

Trial division upto $\sqrt{n}$.

```
bool isPrime (int n) {
    if (n<2) return false;
    for (int i = 2; i*i <= n; i++)
        if (n % i == 0)
            return false;
    return true;
}
```

$O(\sqrt{n})$ by hand just divide by primes 2, 3, 5, 7, etc.

3 divisible → sum of digits divisible by 3

9 divisible → " " " " " 9

$$10^k d_k + 10^{k-1} d_{k-1} + \cdots 10^1 d_1 + 10^0 d_0$$

$$\equiv 1^k \cdot d_k + 1^{k-1} \cdot d_{k-1} + \cdots 1 \cdot d_1 + 1 d_0 \pmod 3 \pmod 9$$

11 divisibility ⇒ alternating digit sum (LUND checksum)

List Primes from 1 to n

```
boolean[] isprime = new boolean[n+1];
Arrays.fill(isprime, true);
isprime[0] = isprime[1] = false;
for (int i = 2; i*i <= n; i++)
    for (int j = 2*i; j <= n; j += i) // 2i, 3i, 4i, 5i
        isprime[j] = false;
```

Inner loop runs $\frac{n}{i}$ times

$$\leq \frac{n}{2} + \frac{n}{3} + \frac{n}{4} + \cdots \frac{n}{n} \sim \boxed{n \ln n}$$

Sum of Divisors

	3^0	3^1	3^2	
2^0	$2^0 3^0$	$2^0 3^1$	$2^0 3^2$	$= 2^0 (3^0 + 3^1 + 3^2)$
2^1	$2^1 3^0$	$2^1 3^1$	$2^1 3^2$	$= 2^1 (3^0 + 3^1 + 3^2)$
2^2	$2^2 3^0$	$2^2 3^1$	$2^2 3^2$	$= 2^2 (3^0 + 3^1 + 3^2)$
2^3	$2^3 3^0$	$2^3 3^1$	$2^3 3^2$	$+ = 2^3 (3^0 + 3^1 + 3^2)$

$$= (2^0 + 2^1 + 2^2 + 2^3)(3^0 + 3^1 + 3^2)$$

$$n = \prod_{p_i \in Primes} p_i^{q_i}$$

$$= \left(\frac{2^4 - 1}{2 - 1}\right) \times \left(\frac{3^2 - 1}{3 - 1}\right)$$

$$\sigma(n) = \prod_{p_i \in Primes} \frac{\left(p_i^{q_i+1} - 1\right)}{(p_i - 1)}$$

Determine the sum of divisors of 225,000 expressing the answer in prime factorized form.

$$225{,}000 = 225 \times 1000$$
$$= 15^2 \times 10^3$$
$$= 3^2 \times 5^2 \times 2^3 \times 5^3 = 2^3 \times 3^2 \times 5^5$$

$$\sigma(225{,}000) = \frac{(2^4-1)}{(2-1)} \times \frac{(3^3-1)}{(3-1)} \times \frac{(5^6-1)}{(5-1)}$$

$$= 3 \times 5 \times 13 \times \frac{(5^3+1)(5^3-1)}{4}$$

$$= 3 \times 5 \times 13 \times \frac{126 \times 124}{4} \quad 31$$

$$= 3 \times 5 \times 13 \times 31 \times 3^2 \times 14$$

$$= \boxed{2 \times 3^3 \times 5 \times 7 \times 13 \times 31}$$

Number of times prime p divides evenly into $n!$

$n! = \underbrace{1 \times 2 \times 3 \times \cdots}_{\text{useless}} \times \underbrace{p}_{1} \times (p+1) \times (p+2) \cdots \times \underbrace{2p}_{2} \cdots \times n$

Cross-offs $\left\lfloor \frac{n}{p} \right\rfloor \rightarrow$ floor (int div)

$\rightarrow 1, 2, 3, \ldots \underset{1}{p}, \ldots \underset{2}{2p}$

new Cross off $\left\lfloor \frac{n}{p^2} \right\rfloor$

times prime p divides evenly into $n!$

$$= \sum_{i=1}^{n} \left\lfloor \frac{n}{p^i} \right\rfloor$$

$n = 937$, $p = 7$

$7 \mid 937$

$7 \mid 133$ R6

$7 \mid 19$

2

$133 + 19 + 2 = 154$

How many ~~does~~ zeroes are at the end of $n!$

$n! = 2^x 5^y \cdots$

$\min(x, y) = y$

→ how many times does 5 divide evenly into $n!$ (same question)

Try $n = 625$

$5 \mid 625$
$5 \mid 125$
$5 \mid 25$
$5 \mid 5$
1

125
25
5
+ 1
156 0's

at end of $625!$

note: 152 0s at end of $624!$