Note Title 10/23/2014

# Mod and Div Functions

The Division Algorithm

For any integer n and any integer $d > 1$, there are unique integers q (quotient) and r (remainder) such that:

$$n = d \cdot q + r \quad \text{and} \quad r \in \{0, 1, \ldots, d-1\}$$

Defines two operations: $n \bmod d = r$
$n \operatorname{div} d = q$.

$53 - 7 \cdot 7 = 4$

$53 \operatorname{div} 7 = 7$ $\qquad$ $32 \operatorname{div} 8 = 4$
$53 \bmod 7 = 4$ $\qquad$ $32 \bmod 8 = 0$

$153 \operatorname{div} 10 = 15$
$153 \bmod 10 = 3$

$-56 \mapsto -45 \mapsto -34 \mapsto -23 \mapsto -12 \mapsto -1 \mapsto 10$

$\Rightarrow$ $-56 \bmod 11 = 10$ $\qquad$ $-17 \bmod 2 = 1$
$-56 \operatorname{div} 11 = -6$ $\qquad$ $-17 \operatorname{div} 2 = -9$

$-56 \bmod 8 = 0$
$-56 \operatorname{div} 8 = -7$

$$n = d \cdot q + r$$
$$-56 = 11 \cdot (-6) + 10$$

$$(k \cdot 11 + 4)^7 \bmod 11$$
$$= 4^7 \bmod 11$$

## Modular Arithmetic:

$$\left((332)^7 + 14 \cdot 72\right) \bmod 11$$

$$\left[\left((332 \bmod 11)^7\right) + (14 \bmod 11)(72 \bmod 11)\right] \bmod 11.$$

$$[2^7 + 3 \cdot 6] \bmod 11 = [128 \bmod 11 + 18 \bmod 11] \bmod 11$$

$$= [7 + 7] \bmod 11 = 3.$$

$\Rightarrow$ In computing arithmetic expressions mod $n$, can take intermediate results mod $n$.

$$(770 \cdot 372) \bmod 7$$

$$= (770 \bmod 7)(\qquad) \bmod 7$$

$$0 \cdot \boxed{\phantom{x}} = 0$$

$$(5631 \cdot 9^{18} + 7) \bmod 2.$$

$$(1 \cdot 1 + 1) \bmod 2 = 2 \bmod 2 = 0.$$

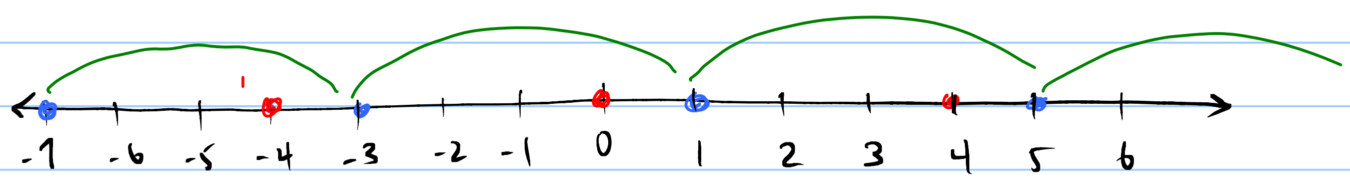
# Equivalence mod n

$x \bmod n = y \bmod n \iff n \mid (x-y)$

in which case "x is equivalent to y mod n".

$x \equiv y \bmod n.$

Equivalence mod 4.




$(5 - -7) = 12$ div by 4.

Equivalence classes mod 4: $-13, 2, 67, 53, -101, 42, 7$

| 0 | 1 | 2 | 3 |
|---|---|---|---|
| | 53 | 2 | −13 |
| | | 42 | 67 |
| | | | −101 |
| | | | 7 |

# The ring $\mathbb{Z}_n$.

Ring is a closed mathematical system with addition and multiplication operations.

Obeys certain laws (e.g. distributive, associative, etc.)

Identity elements:

$$x + 0 = x$$

$$x \cdot 1 = x.$$

Include polynomials, sequences, matrices, etc.

$\mathbb{Z}_n$: integers mod $n$.

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}.$$

| + | 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 |

# Prime Factorization

Every integer greater than 1 is either

prime → only factors are 1 and itself.

composite → has a factor other than 1 or itself.

17, 2, $39 = 3 \cdot 13$

prime, prime, composite

## Fundamental Theorem of Arithmetic

Every positive integer other than 1 can be expressed uniquely as a product of prime numbers where the primes are written in non-decreasing order.

$\Rightarrow 48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 \cdot 2 \cdot 2$

$84 = 2 \cdot 2 \cdot 3 \cdot 7$

Multiplicity of prime p is the # of times it appears in the prime factorization.

Multiplicity of 2 in prime factorization of 48 is 4.

Multiplicity of 7 in p.f. of 84 is 1.

Expontial notation in prime factorization:

each prime appears once — multiplicity in exponent.
primes in increasing order.

$48 = 2^4 \cdot 3$

$84 = 2^2 \cdot 3 \cdot 7$

Computing the prime factorization for a # is hard
(we use small examples).
but once you have it, other things become easy

Let $x$ + $y$ be two integers:

The greatest common divisor of $x$ + $y$ $\gcd(x,y)$
is the largest number that is a factor of $x$ + $y$.

The least common multiple of $x$ + $y$ $\text{lcm}(x,y)$
is the smallest number that is an integer multiple of $x$ + $y$.

$\gcd(48, 36) = 12$

$\gcd(13, 39) = 13$

$\gcd(16, 35) = 1$
(relatively prime)

$\text{lcm}(48, 12) = 48$

$\text{lcm}(\overset{2\cdot 7}{14}, \overset{2^3}{8}) = 7 \cdot 8 = 56$

$\text{lcm}(15, 7) = 105$

$\Rightarrow 532 = 2^2 \cdot 7 \cdot 19$ $\qquad$ $2 \quad 3, \quad 5 \quad 7 \quad 19$

$648 = 2^3 \cdot 3^4$

$1083 = 3 \cdot 19^2$

$\Rightarrow 15435 = 3^2 \cdot 5 \cdot 7^3$

$\gcd(532, 15435)$

$$532 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 19^1$$

$$15435 = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^3 \cdot 19^0$$

$$\gcd = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 19^0 = 7$$

$$\mathrm{lcm} = 2^{\boxed{2}} \cdot 3^2 \cdot 5^1 \cdot 7^3 \cdot 19^1$$

$$\gcd(x,y) \cdot \mathrm{lcm}(x,y) = x \cdot y.$$

Factoring:

Input: integer $N > 1$.

For $X = 2$ to ~~$N-1$~~ $\sqrt{N}$

If $X$ evenly divides $N$ $\Rightarrow$ $10^{-10}$

Return $(X, N/x)$

En-for

Return ("Prime").

End

If $N$ is composite, then it has a factor that is at most $\sqrt{N}$.

$N \sim 200$ digits.

$\sqrt{N} \sim 100$ digits. $10^{100}$

loop takes $10^{-10}$ seconds.

$10^{90}$ seconds : $\sim$ $300 \times 10^{80}$ years.

There is an efficient algorithm for primality testing:

**Factoring**

Input: integer $N > 1$.

Output: If $N$ is prime $\rightarrow$ "Prime"

If $N$ is composite $\rightarrow$ $x$ and $y$ integers. $x \cdot y = N$.

Hard

**Primality Testing**

Input: integer $N > 1$.

Output: If $N$ is prime $\rightarrow$ "Prime"

If $N$ is composite $\rightarrow$ "Composite".

Easy.

$(\#\text{ digits})^{12}$ ~ small power.

# Finding Primes:

Are there large primes?

Euclid showed in 300 B.C. :

There are an infinite number of primes.

Try this: Repeat until success:

Pick a random 200 digit number. p.
Test if p is prime
If yes, return (p).
If no, continue.

What is the likelihood of success.

To answer this question, we need to know the density of primes among 200 digit numbers.

This doesn't quite do it, but it's close:

Prime Number Theorem:

Let $\pi(x)$ be the number of prime numbers in the range from 2 to x:

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

A randomly chosen number in the range from $2 \ldots x$ is prime with probability $\frac{1}{\ln(x)}$.

$\Rightarrow$ It takes on average $\ln(x)$ trials to find a prime number in the range from $2 \ldots x$.

$x$ is 200 digits: $\ln(x) \approx 200 \cdot \ln(10)$
$\approx 460$