Primes

Monday, March 30, 2026 11:44 AM

Recall: Modular Arithmetic

Missing
700# 4, (20), 22
800# 20

1] Exer:

$$1526 \times 346 \pmod 3$$
$$\equiv 2 \cdot 1$$
$$\equiv 2 \pmod 3$$

Exer:

$$1789 \times 332 \pmod 3$$
$$\equiv 1 \times 2 \equiv 2 \pmod 3$$

2] Primes: (§ 4.3)

Def^n. $n > 1$ is prime if it has exactly two positive divisors: 1 and n.

Otherwise n is called composite.

3] The Fundamental Theorem of Arithmetic (FTA)

Thm: every integer > 1 can be written uniquely as a prime or a product of primes.

e.g. $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

$105 = 3 \cdot 5 \cdot 7$

$81 = 3^4$

$97 = 97$

$1024 = 2^{10}$

4] Thm: a composite n has a prime divisor $\leq \sqrt{n}$

4] Thm: a composite n has a prime divisor $\leq \sqrt{n}$

e.g. Show that 103 is a prime

Sol^n. it is not divisible by $2, 3, 5, 7 \leq \sqrt{103}$

5] Thm: There are infinitely many primes.

Proof: assume that there finitely many primes:

$$p_1, p_2, p_3, \ldots, p_n$$

let $q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$

then for $p_i \nmid q$ for $i = 1, 2, \ldots, n$

$\Rightarrow$ q is a new prime or divisible by new primes by FTA.

This contradicts the assumption of having n primes.

$\therefore$ there are infinitely many primes

6] Mersenne Primes:

a prime of the form $2^p - 1$ for prime p.

otherwise, $2^p - 1$ is called Mersenne composite.

e.g.

$2^p - 1$

$2^3 - 1 = 7$ ✓

$2^5 - 1 = 31$ ✓

$2^7 - 1 = 127$ ✓

$2^{11} - 1 = 2047 = 23 \times 89$ (not prime)

7] Thm: Number of primes $\leq n$ is

$$\pi(n) \cong \frac{n}{\ln(n) - 1}$$

8] The greatest common divisor (§ 4.3)

$\gcd(a, b) = d$ is the greatest integer s.t. $d \mid a$ and $d \mid b$.

e.g.

$\gcd(24, 36) = 12$

$\gcd(15, 22) = 1 \Longrightarrow$ 15 and 22 are relatively prime (co-prime)

9] Def^n. a and b are relatively prime (or co-prime) if $\gcd(a, b) = 1$

10] Least Common multiple: (§ 4.3)

The $lcm(a, b)$ is the smallest m s.t $a \mid m$ and $b \mid m$.

e.g. $lcm(24, 36) = 72$

$lcm(14, 15) = 210$

$lcm(8, 16) = 16$

11] How to find lcm / gcd by factorization

by FTA: let $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$

$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$

$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots$

$\text{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_2)} p_2^{\max(\alpha_2,\beta_2)} \cdots$

e.g.

$a = 24 = 2^3 \cdot 3^1$

$b = 36 = 2^2 \cdot 3^2$

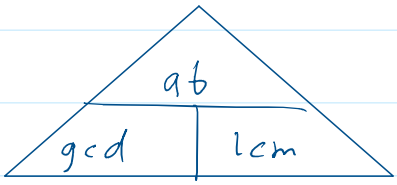
$\gcd(a,b) = 2^2 \cdot 3^1 = 12$

$\text{lcm}(a,b) = 2^3 \cdot 3^2$

$= 8 \cdot 9 = 72$

12] Thm:

$$\gcd(a,b) \cdot \text{lcm}(a,b) = a \cdot b$$



13] Integer Representation (§ 4.2)

Thm: The base-b expansion of integer $n \in \mathbb{Z}^+$, n can be written uniquely it the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0$$

where a_i are digits in base b, $0 \le a_i < b$

Notation: $n = (a_k a_{k-1} a_{k-2} \cdots a_1 a_0)_b$ in base b

e.g. 1527 in base 10 (by default)

$= 1 \times 10^3 + 5 \times 10^2 + 2 \times 10^1 + 7$

14] Binary Expansion $b = 2$

$(1011)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1$

$= 8 + 0 + 2 + 1$

$= 11$

	(8)	(4)	(2)	(1)
3 =	0	0	1	1
6 =	0	1	1	0
9 =	1	0	0	1
A =	1	0	1	0
B =	1	0	1	1
C =	1	1	0	0
F =	1	1	1	1

15] Hexadecimal Expansion : $b = 16$ (Hex)

using 0—9, A—F for 0—15

$(2AF)_{16} = 2 \cdot 16^2 + 10 \cdot 16^1 + 15$

16] Base - conversion

to put n in base b, div n by b

$n = \underline{q_0} \cdot b + \underline{r_0}$ $\quad 0 \leq r_i < b$

$q_0 = \underline{q_1} \cdot b + \underline{r_1}$

$\vdots$

$q_k = \underline{q_k} \cdot b + \underline{r_k}$

$\Rightarrow (r_k \; r_{k-1} \; \cdots \; r_0)_b = n$

17] e.g. Put 37 in binary (base 2)

$37 = 18 \cdot 2 + 1$

$18 = 9 \cdot 2 + 0$

$9 = 4 \cdot 2 + 1$

$4 = 2 \cdot 2 + 0$

$2 = 1 \cdot 2 + 0$

$1 = 0 \cdot 2 + 1$

read it backwards

$\Rightarrow (100101)_2 = 37$

$32 + 4 + 1 = 37$