Math 321

Q5

(a) $(1,2,3)_{10} = (\quad)_6 = (\quad 3\ ,2,3)_6$

$(1,2,3)_6 = (\quad)_{10}(6)_{10} + (\ 3\ )_{10}$

$(7,0)_{10} = (\ 3\ )_{10}(6)_{10} + (\ 2\ )_{10}$

$(3)_{10} = (\ 0\ )_{10}(6)_{10} + (\ 3\ )_{10}$

check: $3\cdot 36 + 2\cdot 6 + 3$

$108 + 12 + 3$

123

$(1,2,5)_8 = (\quad)_9 = (\ 2\ ,1,5)_9$

$(1,2,5)_8 = (1,5)_8(9)_8 + (5)_8$

$8(1) + 8(9)^8(2) = 8(5,1)$

$8(2) + 8(9)8(0) = 8(2)$

4.2 # $3^{2003} \pmod{99} =$

$(2003)_{10} = (1,1,1,1,1,0,1,0,0,1,1)_2$

$2003 = (1001)2 + 1$

$1001 = (500)2 + 1$

$500 = (250)2 + 0$

$250 = (125)2 + 0$

$125 = (62)2 + 1$

$62 = (31)2 + 0$

$31 = (15)2 + 1$

$15 = (7)2 + 1$

$7 = (3)2 + 1$

$3 = (1)2 + 1$

$1 = (0)2 + 1$

(continued)

$3^{2003} \bmod 99 = 3^{(1,1,1,1,1,0,1,0,0,1,1)_2} \bmod 99$

$(2003)_{10} = (1,1,1,1,1,0,1,0,0,1,1)_2$

$(81)^1 (9)^1 (36)^1 (27)^1 (81)^1 (9)^0 (36)^1 (27)^0 (81)^0 (9)^1 (3)^1 \bmod 99$

$1296 \bmod 99$, $6561 \bmod 99$, $729 \bmod 99$

ans = 3

ans = ans · 9 = 27

ans = ans · 36 =

$(81)^1 (9)^1 (36)^1 (27)^1 (81)^1 (9)^0 (36)^1 (27)^0 (81)^0 (9)^1 (3)^1 \bmod 99$

27, 81, 9, 36, 27, $972 \bmod 99 = 81$, 27

Fund. Thm $n \geq 2$ is prime or a unique prod of primes (in non-dec order)

Thm If c is composite it has a prime factor $\leq \sqrt{n}$.

(Ex) is 103 prime? primes: 2, 3, 5, 7, 11 ($\sqrt{103} \approx 10$)

$7 \overline{)103}$ R 5 (14, 7, 33, 28, 5) $7 \nmid 103$ so 103 is prime

---

Thm There are infinitely many primes

Pf assume primes are finite. we have k primes. Primes $= \{p_1, p_2, p_3, p_4, \ldots, p_k\}$

Consider: $P = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1$

by fund. thm P has a prime divisor. call it p_*

$p_* \mid P$ and $p_* \mid (p_1 \cdot p_2 \cdot \dots \cdot p_k)$

then: $p_* \mid P - (p_1 \cdot p_2 \cdot \dots \cdot p_k)$

$p_* \mid 1 \equiv \not\exists$

Infinite primes but how rare are they?

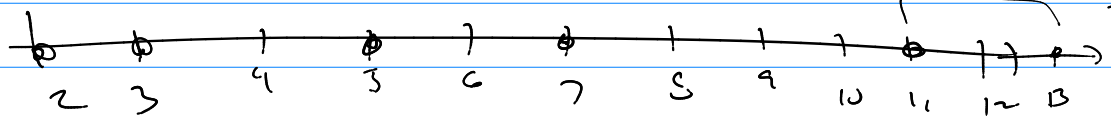
$\pi(n)$ = count # of primes from 2 to n

$\pi(2) = 1$ $\quad \pi(5) = 3$ $\quad \pi(8) = 4$ $\quad \pi(11) = 5$

$\pi(3) = 2$ $\quad \pi(6) = 3$ $\quad \pi(9) = 4$

$\pi(4) = 2$ $\quad \pi(7) = 4$ $\quad \pi(10) = 4$

$\frac{\pi(12)}{12} = \frac{5}{12}$



$\pi(n) \approx \frac{n}{\ln(n)}$ $\quad \lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1$

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

② & $\frac{\pi(n)}{n} \sim \frac{n/\ln n}{n} = \frac{1}{\ln n}$ $\quad \lim_{n\to\infty} \frac{1}{\ln n} = 0$

Applications & Primes:

① Prime Factorization $\quad 106 = 2 \cdot 53$

2 $\quad$ 53

② GCD / lcm

gcd(a,b) is the largest d such that $d \mid a \wedge d \mid b$

lcm(a,b) is the smallest m such that $a \cdot k_1 = m \wedge b \cdot k_2 = m$

by $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ $\quad b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)}$$
$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_k^{\max(a_k,b_k)}$$

So.. $ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$

(ex) $a = 2^2 3^0 5^1 7^3$ $\quad b = 2^0 3^1 5^2 7^2$

$\gcd = \boxed{2^0 3^0 5^1 7^2}$

$\operatorname{lcm} = \boxed{2^2 3^1 5^2 7^3}$

Finding gcd by Euclidean Algorithm.

$a = q \cdot b + r$ $\quad 0 \le r < b$ $\quad \gcd(a,b) = \gcd(b,r)$

$= \gcd(123, 21)$ $\quad 123 = (5)21 + (18)$ $\quad 3 = (1)21 + (-1)18$

$= \gcd(21, 18)$ $\quad 21 = (1)18 + (3)$ $\quad 3 = (1)21 + (-1)[123 - 5 \cdot 21]$

$\gcd(18, 3) = 3$ $\quad 18 = (6)3 + (0)$ $\quad 3 = (6)21 + (-1)123$

Bezout's Identity $\quad \gcd(a,b) = s \cdot a + t \cdot b$

Why? (1) $\gcd(a,b) = 1$ we say a,b are relatively prime.

(2) by Bezout's $\quad 1 = s \cdot a + t \cdot b$

(3) $(1) \bmod b = (s \cdot a + t \cdot b) \bmod b$

$(1) \bmod b = (s \cdot a) \bmod b + (t \cdot b) \bmod b$

$1 = (s \cdot a) \bmod b + 0$

$1 = (s \cdot a) \bmod b$ or $s \cdot a \underset{b}{\equiv} 1$

↑ So s is a's mult. inverse under mod b.

So if a, b are relatively prime then a has an inverse under mod b.

(ex) $3 \cdot ? \ (\bmod 7) = 1$

$\ldots \equiv -13 \equiv -6 \equiv 1 \equiv 8 \equiv 15 \equiv 22 \equiv 29 \equiv \ldots$ (mod 7)

$\gcd(7,3)$ $\quad 7 = (2)3 + (1)$ → $\quad 1 = (1)(7) + (-2)(3)$

$\gcd(3,1) = 1$ $\quad 3 = (3)1 + (0)$

↑ 3's inv. under mod 7

3's inv. $= -2 \equiv 5 \equiv 12 \ldots$ (mod 7)