Homework 20-22

Wednesday, April 7, 2021 7:04 PM

"I pledge my honor I have abided by the Stevens Honor system."

- Alex Gaskins

Problem 20.1. a) Use Euclidean algorithm and Bezout's identity to compute 21^{-1} modulo 101. Show your work.

$101 = 21(4) + 17$

$21 = 17 + 4$

$17 = 4(4) + 1$

$1 = 17 - 4(4)$

$1 = (101 - 21(4)) - 4(21 - 17)$

$1 = (101 - 21(4)) - 4(21) + (4(17))$

$1 = 101 \underline{-8}(21) + 4(17)$

$$\boxed{21^{-1} \bmod 101 = -8 \quad \text{or} \quad [101 - 8] = 93}$$

b) Solve the congruence $21y \equiv 8 \pmod{101}$. Show your work.

$21y \equiv 8 \pmod{101}$

$\gcd(21, 101) = 1$ ✓

$8 = 21y - 101k$

$8 = 21(10) - 101(2)$

$\boxed{y = 10}$

Problem 21.1. a) Prove that there exists a natural n such that

$$\begin{cases} 2n \equiv 3 \pmod{11} \\ 5^n \equiv 125 \pmod{2021} \\ n \equiv 10 \pmod{19} \end{cases}.$$

$\gcd(2, 11) = 1$

$\gcd(5, 2021) = 1$ ✓

$\gcd(1, 19) = 1$

$2n \equiv 3 \bmod 11$

$11 - 2(5) \equiv 1$

$2(5) \equiv 1 \bmod 11$

$5^n = 125 \bmod 2021$

$125 \bmod 2021 = 125 - 2021(0)$

$= 125$

$2(5) \equiv 1 \bmod 11$

$2(5(3)) \equiv 3 \bmod 11$

$2(15) \equiv 3 \bmod 11$

$\boxed{n = 15}$

$= 125$

$= 5^3$

$\boxed{n = 3}$

$n = 10 \bmod 19$

$10 \bmod 19 = 10 - 19(0)$

$\boxed{n = 10}$

b) Find an integer n that satisfies the first two equations above.

$(2(5) = 10 \bmod 11 = 1 \bmod 11)$

$2n \equiv 3 \bmod 11 = n \equiv 4 \bmod 11$

$5^n \equiv 125 \bmod 2021 \quad n \equiv \log_5(125)\ [\bmod 2021] = n \equiv 3 \bmod 2021$

Both sides are divisible by 5

$n = 2021(6)\underbrace{[\bmod 11]}_{4 \bmod 11} + \underbrace{11(184)\ [\bmod 2021]}_{3 \bmod 2021}$

$n = 2021(6) + 11(184)$

$\boxed{n = 14,150}$

c) (*bonus 2 points*) Find an integer n that satisfies all 3 equation above.

$n = 4 \bmod 11 \quad n = 3 \bmod 2021 \quad n = 10 \bmod 19$

$$2021(19) + 19(11) + 2021(11)$$

$$38399\,[\text{mod } 11] + 209\,[\text{mod } 2021] + 22231\,[\text{mod } 19]$$

9 ↓ 4 mod 11 ↓ 3 mod 2021 ↓ 10 mod 19

$$\boxed{n = 347615}$$

Problem 22.1. Prove that there are infinitely many prime numbers of the form $4l + 3$ for some integer l by following the next steps:

a) Prove by induction on k that if $n = p_1 \cdot p_2 \cdots p_k$ and $p_i \equiv 1 \pmod 4$, then $n \equiv 1 \pmod 4$.

If $n = 1$ then $n = p_1$ and $p_1 \equiv 1 \bmod 4$

so $n \equiv 1 \bmod 4$

For $k = r$, $k = r+1$ where $n = p_1 p_2 \cdots p_{r+1}$

$p_1 p_2 \cdots p_r = 1 \bmod 4$ because the result is true for $k = r$

So $p_1 p_2 \cdots p_r = 4a + 1$ where $a \in N$

$p_{r+1} = 4b + 1$ where $b \in N$

$$n = (p_1 p_2 \cdots p_r)\, p_{r+1} = (4a+1)(4b+1) = 16ab + 4a + 4b + 1 \equiv 1 \bmod 4$$

$\therefore$ True for $k = r+1$

b) Use prime power decomposition to prove that if $n \equiv 3 \pmod 4$ then n has a prime divisor of the form $4l + 3$ for some integer l.

$n \equiv 3 \mod 4$

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$

If $p_i \equiv 1 \mod 4$ for all i then

$p_i^{\alpha_i} \equiv 1 \mod 4 \quad \forall i$

$\prod_{i=1}^{n} p_i^{\alpha_i} \equiv 1 \mod 4 \rightarrow n \equiv 1 \mod 4$

is invalid

so there exists a p_i where $p_i \equiv 3 \mod 4$

and n has a prime factor in the form of $4l+3$

c) Prove that there are infinitely many prime numbers of the form $4l + 3$

Let $p_1, p_2, \ldots p_r$ be prime numbers in the form $4l+3$

Meaning $\equiv 3 \mod 4$

Let $N = 4p_1p_2 \cdots p_r - 1$ where $N > 1$ and N is odd

$N \equiv -1 \equiv 3 \mod 4$ where N has a prime divisor p_{r+1} in the form $4l+3$

$\therefore$ There are infinitely many prime numbers in the form $4l+3$.