

problem 1. 1. (24 points). Find, with proof, all integers x with $0 \leq x \leq 301$ with

$$21x \equiv 161 \pmod{301}$$

Do not use a calculator on this problem.

Proof.

$$\begin{aligned} 21x \equiv 161 \pmod{301} &\iff 15 \cdot 21x \equiv 15 \cdot 161 \equiv 2415 \pmod{301} \\ &\iff 305x \equiv 2415 \pmod{301} \\ &\iff 4x \equiv 7 \pmod{301} \\ &\iff 4 \cdot 75x \equiv 7 \cdot 75 \pmod{301} \\ &\iff -x \equiv 224 \pmod{301} \\ &\iff x \equiv 77 \pmod{301} \end{aligned}$$

because $0 \leq x \leq 301$, so $x = 77$ ■

problem 2. 2. (24 points). Find the smallest positive integer r so that

$$111^{94} \equiv r \pmod{79}$$

You may not use a calculator, but you may use the fact that 79 is prime.

Proof.

$$\begin{aligned} 114^{94} &\equiv r \pmod{79} \\ \Rightarrow r &\equiv (35)^{94} \pmod{79} \end{aligned}$$

becomse 79 is a prime. So by farmat litte theorem

$$(35)^{78} \equiv 1 \pmod{79}$$

so $r \equiv 35^{16} \equiv (1125)^8 \equiv (1125 - 1106)^8 \equiv 19^8 \equiv 36^4 \equiv 45^4 \equiv 2025^2 \pmod{79}$.

We know $2025 \equiv 2025 - 79 \cdot 25 \equiv 2025 - 1975 \equiv 50 \pmod{79}$

So $r \equiv 50^2 \equiv 2500 \equiv 2500 - 31 \cdot 79 \equiv 2500 - 2449 \equiv 51 \pmod{79}$

So the mallest positive integer so that $111^{94} \equiv r \pmod{79}$ is $r = 51$. ■

problem 3. 3. (24 points). Find the unique positive integer n with $1 \leq n \leq 1000$ so that

$$\begin{aligned} n &\equiv 2 \pmod{7} \\ n &\equiv 3 \pmod{11} \\ n &\equiv 5 \pmod{13}. \end{aligned}$$

Do not use a calculator.

Proof. If we can find x, y, z satisfied

$$\begin{cases} 11 \cdot 13 \cdot x \equiv 1 \pmod{7} \\ 7 \cdot 13 \cdot y \equiv 1 \pmod{11} \\ 7 \cdot 11z \equiv 1 \pmod{13} \end{cases}$$

and take $n \equiv 2 \cdot 11 \cdot 13 \cdot x + 3 \cdot 7 \cdot 13 \cdot y + 5 \cdot 7 \cdot 11 \cdot z \pmod{7 \cdot 11 \cdot 13}$

then it is easy to check $\begin{cases} n \equiv 2 \pmod{7} \\ n \equiv 3 \pmod{11} \\ n \equiv 5 \pmod{13} \end{cases}$

So the problem reduce to find x, y, z

in fact $x \cdot 143 \equiv 1 \pmod{7} \Rightarrow 3 \cdot x \equiv 1 \pmod{7} \Rightarrow x \equiv 5 \pmod{7}$

$y \cdot 91 \equiv 1 \pmod{11} \Rightarrow 3y \equiv 1 \pmod{11} \Rightarrow y \equiv 4 \pmod{11}$

$z \cdot 77 \equiv 1 \pmod{13} \Rightarrow 12 \cdot z \equiv 1 \pmod{13} \Rightarrow z \equiv 12 \pmod{13}$

So when $n \equiv 2 \cdot 11 \cdot 13 \cdot 5 + 3 \cdot 7 \cdot 13 \cdot 4 + 5 \cdot 7 \cdot 11 \cdot 12 \equiv 7142 \equiv 135 \pmod{1001}$
we know n satisfied the condition, so $n = 135$ is the unique positive number n satisfied the condition

■

problem 4. 4. (24 points). Let $d = \gcd(2528^{2767} - 1, 4072^{1601} - 1)$. Prove that if q is a prime divisor of d , then $q \equiv 1 \pmod{2767 \cdot 1601}$. You may use that $\gcd(2527, 4071) = 1$ and that 2767 and 1601 are primes, but do not use a calculator or computer for computations.

Proof. assume $2767 = p_1$ $1601 = p_2$ $2527 = x$ $4071 = y$

how q is a prime and $q \mid (x+1)^{p_1} - 1$, $q \mid (y+1)^{p_2} - 1$ because $g(d(x, y)) = 1$
so $q \mid x, q \mid y$ can not hold at the same time.

Case A $(q, xy) = 1$, in this case, we prove $q \equiv 1 \pmod{p_1 p_2}$.

in fact, consider a is the smallest integer s.t. $q \mid x^a - 1$, because $(q, x) = 1$, so $a \geq 2$, now, $q \mid x^a - 1, q \mid x^{p_1} - 1$, so we have $q \mid x^{\gcd(a, p_1)} - 1$.

because $\gcd(p, a) \leq \min\{ap_1\}$ and by the choose of a we know $p_1 = a$.

and on the other hand by farmat little theorem, $d \mid x^{d-1} - 1$ (because d is a prime).
so $p_1 \mid d-1$ i.e. $d \equiv 1 \pmod{p_1}$ by the same argument we know $d \equiv 1 \pmod{p_2}$,
so $d \equiv 1 \pmod{p_1 p_2}$

Case B. $q \mid x$ or $q \mid y$ in this case there exist counterexample we can only prove $d \equiv 1 \pmod{p_1}$ or $d \equiv 1 \pmod{p_2}$

■

problem 5. 5. (24 points). Let k be a positive integer. Prove that there is some positive integer n so that $k \cdot 3^n + 1$ is composite.

Proof. assume there do not exist positive number n so that $k \cdot 3^n + 1$ is composite. then for all $n \in \mathbb{N}^*$. $k \cdot 3^n + 1$ is a prime. now arbitrarily choose a positive number $n_0 \in \mathbb{N}^*$ and assume $k \cdot 3^{n_0} + 1 = p_0$. p_0 is a prime.

then $(3, p_0) = (3, k \cdot 3^{n_0} + 1) = (3, 1) = 1$ so by Fermat's little theorem

$$3^{p_0-1} \equiv 1 \pmod{p_0}$$

so

$$k \cdot 3^{n_0+p_0-1} + 1 \equiv k \cdot 3^{n_0} \cdot 3^{p_0-1} + 1 \equiv k \cdot 3^{n_0} + 1 \equiv 0 \pmod{p_0}$$

i.e. $p_0 | k \cdot 3^{n_0+p_0-1} + 1$. but $p_0 = k \cdot 3^{n_0} + 1 < k \cdot 3^{n_0+p_0-1} + 1$. So $k \cdot 3^{n_0+p_0-1} + 1$ is composite. this contradicts with the previous assumption so there exist some positive integer n . so that $k \cdot 3^n + 1$ is composite. ■