Number Theory Exercises

(solutions at the end)

① Find all $n \in \mathbb{N}$ with $n \geq 1$ and $(n+1) \mid (n^2+1)$.

From the book "250 problems in elementary number theory"

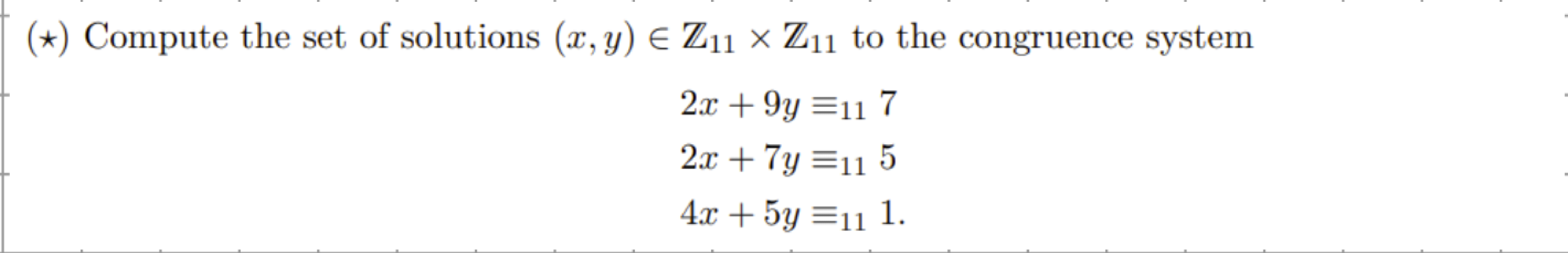
Option 1: - Remember the definition of $x \mid y$
- for all x, y either $x < y$, $x = y$ or $x > y$

Option 2 : - Remember that $a + 0 = a$ and $0 = n - n$

② Prove that $\gcd(a, \gcd(b,c)) = \gcd(\gcd(a,b), c)$

Hint: Use the prime number definition of gcd.

③



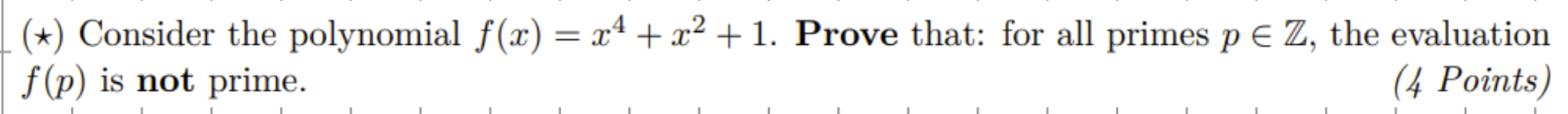
(⋆) Compute the set of solutions $(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11}$ to the congruence system

$$2x + 9y \equiv_{11} 7$$
$$2x + 7y \equiv_{11} 5$$
$$4x + 5y \equiv_{11} 1.$$

From the HS24 exam.

Hint: Just treat them like you treated normal equations in school.

④



(⋆) Consider the polynomial $f(x) = x^4 + x^2 + 1$. **Prove** that: for all primes $p \in \mathbb{Z}$, the evaluation $f(p)$ is **not** prime. *(4 Points)*

From the HS24 exam.

Option 1: - Remember that each number is either $3k+0$, $3k+1$ or $3k+2$ for some k. So $x \equiv_3 0$ or $x \equiv_3 1$ or $x \equiv_3 2$.

Option 2 : - Remember that $0 = x^2 - x^2$
- Remember that $(a+b)^2 = a^2 + 2ab + b^2$
- Remember that $a^2 - b^2 = (a-b)(a+b)$

SOLUTIONS:

1 Option 1: Say that $n+1 \mid n^2+1$. Then there exists x such that $x(n+1) = n^2+1$.
Now we do a case distinction:

a) $x > n$: Then $x(n+1) > n(n+1) = n^2+n$.
This means $n^2+1 > n^2+n$
$\Rightarrow 1 > n$, but we want $n \geq 1$

b) $x < n$: Then $x \leq n-1$ and $x(n+1) \leq (n-1)(n+1) = n^2-1$.
This means $n^2+1 \leq n^2-1$
$\Rightarrow 1 \leq -1$, a contradiction

c) $x = n$: Then $x(n+1) = n(n+1) = n^2+n$.
This means $n^2+n = n^2+1$
$\Rightarrow n = 1$

So 1 is the only solution.

Option 2: We use the fact that $n-n=0$:

$$n^2+1 = n^2+1+0 = n^2+1+n-n = n^2+n-(n-1) = n(n+1)-(n-1)$$

So if $(n+1) \mid (n^2+1)$ then $(n+1) \mid (n-1)$, since it already divides $n(n+1)$. But since $n+1 > n-1$ this only holds for $n-1=0$ and so only for $n=1$.

② Say $a = \prod_i p_i^{\alpha_i}$, $b = \prod_i p_i^{\beta_i}$, $c = \prod_i p_i^{\gamma_i}$.

Then $\gcd(b,c) = \prod_i p_i^{\min(\beta_i, \gamma_i)}$.

And so $\gcd(a, \gcd(b,c)) = \prod_i p_i^{\min(\alpha_i, \min(\beta_i, \gamma_i))}$.

A similar argument shows that $\gcd(\gcd(a,b),c) = \prod_i p_i^{\min(\min(\alpha_i, \beta_i), \gamma_i)}$.

To show that they are equal we show that:

$$\min(x, \min(y,z)) = \min(\min(x,y), z) \quad \text{for all } x, y, z.$$

We do a case distinction:

a) $x \leq y \wedge x \leq z$: Then $x \leq \min(y,z)$ since $\min(y,z)$ is either y or z and so the LHS is x.
Also $\min(x,y) = x$ and $\min(x,z) = x$ so the RHS is also x.

b) $y \leq x \wedge y \leq z$
c) $z \leq x \wedge z \leq y$ follow similar arguments.

Since we can order the numbers, one of them has to be first in the ordering, so one of the cases must apply.

We showed that $\min(\alpha_i, \min(\beta_i, \gamma_i)) = \min(\min(\alpha_i, \beta_i), \gamma_i)$

$$\Rightarrow \prod_i p_i^{\min(\alpha_i, \min(\beta_i, \gamma_i))} = \prod_i p_i^{\min(\min(\alpha_i, \beta_i), \gamma_i)}$$

$$\Rightarrow \gcd(a, \gcd(b,c)) = \gcd(\gcd(a,b), c)$$

We showed that the magma $(\mathbb{N}, \gcd)$ is actually a semigroup!

③ We have
$$2x + 9y \equiv_{11} 7 \quad ①$$
$$2x + 7y \equiv_{11} 5 \quad ②$$
$$4x + 5y \equiv_{11} 1 \quad ③$$

Subtracting ①-② gives $2y \equiv_{11} 2$ and so $y \equiv_{11} 1$.

Substituting into ③ gives $4x + 5 \equiv_{11} 1$

$\Rightarrow 4x \equiv_{11} -4$

$\Rightarrow x \equiv_{11} -1$

$\Rightarrow x \equiv_{11} 10$ (+11 on both sides)

So $x = 10$ and $y = 1$

④

Option 1: We do a case distinction:

a) $R_3(p) = 0$. The only prime for which this holds is 3 (since if $R_3(p) = 0$ then it is divisible by 3).
We see that $f(3) = 3^4 + 3^2 + 1 = 81 + 9 + 1 = 91 = 7 \cdot 13$

b) $R_3(p) = 1$. Then $R_3(f(p)) = R_3(p^4 + p^2 + 1)$
$= R_3(R_3(p)^4 + R_3(p)^2 + 1)$
$= R_3(1^4 + 1^2 + 1)$
$= R_3(3) = 0$

and so $f(p)$ is divisible by 3.

c) $R_3(p) = 1$. Then $R_3(f(p)) = R_3(p^4 + p^2 + 1)$
$= R_3(R_3(p)^4 + R_3(p)^2 + 1)$
$= R_3(2^4 + 2^2 + 1)$
$= R_3(16 + 4 + 1)$
$= R_3(21) = 0$

and so $f(p)$ is divisible by 3.

In all cases $f(p)$ is not a prime.

Fun fact: I managed to miscalculate one of the cases during the exam and tried until modulo 5 until I realized I was wasting time.

Option 2 by Jeferson Morales Mariciano:

$$\begin{aligned} f(x) &= x^4 + x^2 + 1 \\ &= x^4 + x^2 + 1 + (x^2 - x^2) \\ &= x^4 + 2x^2 + 1 - x^2 \\ &= (x^2+1)^2 - x^2 \\ &= ((x^2+1) - x) \cdot ((x^2+1) + x) \end{aligned}$$

So it is a composite number, and therefore not prime.
(Only for $x=1$ we get $f(1)=3$, but 1 is not a prime.)