Homework:
Number theory 2025
deadline 26th November 2025

Instruction: Hand in only as a hard paper copy (no emails) during Wednesday lecture. Keep one copy for yourself.

(i) We have Diophantine equation

$$319x + 473y = k\,,$$

where k is an integer.

(a) For what k there is a solution of this equation?

(b) Find all solutions for $k = 33$.

(ii) Show that all solutions of congruence equation

$$ax \equiv 0\,(mod\,n)$$

are

$$x = k \cdot \frac{n}{gcd(a,n)}\,, \qquad k \in \mathbb{Z}\,.$$

(iii) We have congruence relation

$$3x \equiv p\,(mod\,5)\,,$$

where $p \in \mathbb{Z}$ is a parameter.

(a) For what value p is there a solution?

(b) Find all solutions if $p = 2^{154}$.

(iv) Find criteria for divisibility by 7.

(v) Let p and q be primes. Show that for all $j, l \in \mathbb{N}$

$$(a) \quad p|q^j \Rightarrow p = q$$

$$(b) \quad p^j \perp q^l \text{ whenever } p \neq q\,.$$

Solutions

(i) We have Diophantine equation

$$319x + 473y = k\,,$$

where k is an integer.

(a) For what k there is a solution of this equation?
(b) Find all solutions for $k = 33$

Solution (a)
Euclid algorithm:

$$473 = 1 \cdot 319 + 154$$
$$319 = 2 \cdot 154 + 11$$
$$154 = 14 \cdot 11 + 0\,.$$

It follows that $gcd(319, 473) = 11$. So necessary and sufficient condition for the existence of solution is that:

$$k = 11m\,, m \in \mathbb{N}\,.$$

Solution (b):

We can extract from Euclid algorithm that

$$11 = 319 - 2 \cdot 154 = 319 - 2(473 - 319) = 3 \cdot 319 - 2 \cdot 473\,.$$

Then

$$3 \cdot 319 - 2 \cdot 473 = 11 \quad | \cdot 3$$

$$9 \cdot 319 - 6 \cdot 473 = 33\,.$$

Particular solution is $x = 9, y = -6$.

Solution of homogeneous equation:

$$x = \frac{473}{11} l = 43l\,,$$
$$y = -\frac{319}{11} l = -29l\,,$$

where $l \in \mathbb{Z}$.

Solution:

$$x = 9 + 43\,l$$
$$y = -6 - 29\,l\,.$$

$l \in \mathbb{Z}$.

(ii) Show that all solutions of congruence equation

$$ax \equiv 0 \, (mod \, n)$$

are

$$x = \frac{n}{gcd(a,n)} \cdot k \, , \qquad k \in \mathbb{Z} \, .$$

Solution: p. 21-22, Lecture notes Number theory

(iii) We have congruence relation

$$3x \equiv p \, (mod \, 5) \, ,$$

where $p \in \mathbb{Z}$ is a parameter.

(a) For what value p is there a solution?

(b) Find all solutions if $p = 2^{154}$.

Solution:

(a) Equivalent Diophantine equation is

$$3x + 5y = p \, ,$$

Solution exits if and only if $gcd(3, 5)|p$. As 3 and 5 are coprime we see that equation has solution for all p.

(b) Let us solve equation

$$3x + 5y = 2^{154} \, .$$

We have that $5 = 3+2$ and $3 = 2+1$, giving us conclusion $1 = 2 \cdot 3 - 1 \cdot 5$. Multiply this equation by 2^{154}. We obtain $2^{154} = 3 \cdot 2^{155} - 2^{154} \cdot 5$. So particular solution is

$$x = 2^{155} \, .$$

By problem (iii) we have that all solutions are of the form

$$x = 2^{155} + 5k \, , k \in \mathbb{Z} \, .$$

(iv) Find criteria for divisibility by 7.

Solution: Let

$$a = (a_k a_{k-1} \dots a_1 a_0)_{10} = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0 \,.$$

We have congruence relations

$$10 \equiv 3 \,(mod\, 7) \,.$$

$$10^2 \equiv 3^2 (mod\, 7) \equiv (-1)(mod\, 7)$$

$$10^{2i} \equiv (-1)^i (mod\, 7)$$

$$10^{2i+1} \equiv (-1)^i 10 \cdot 10 \,(mod\, 7) \equiv (-1)^i 3 \,(mod\, 7)$$

Therefore

$$a \equiv a_0 \,(mod\, 7) + 3a_1 - a_2 - 3a_3 + a_4 + 3a_5 - a_6 \cdots =$$
$$= a_0 \,(mod\, 7) + 3(a_1 - a_3 + a_5 - \cdots) - a_2 + a_4 - a_6 + a_8 - \cdots$$

So 7 divides a if and only if 7 divides the following number:

$$a_0 \,(mod\, 7) + 3(a_1 - a_3 + a_5 - \cdots) - a_2 + a_4 - a_6 + a_8 - \cdots$$

(v) Let p and q be primes. Show that for all $j, l \in \mathbb{N}$

$$(a) \quad p|q^j \Rightarrow p = q$$

$$(b) \quad p^j \perp q^l \text{ whenever } p \neq q\,.$$

Solution: (a)

By the property of primes (see the lecture).

$$p|a_1 a_2 \cdots a_n \Rightarrow p|a_i \text{ for some } i.$$

So as p divides q^l we have that $p|q$. Therefore $p = q$.

(b) Suppose that $a|p^j$ and $a > 1$. Then by the uniqueness of prime number decompositions we have that $a = p^i$ for some $i \leq j$. Suppose that $a|q^l$. Then $p|q^l$ and so $p|q$ by the property of prime numbers. But then $p = q$ which is a contradiction. Therefore $\gcd(p^j, q^i) = 1$.