Math 402 Homework 1

Alexandre Lipson

January 15, 2025

Problem (1)**.** Prove $\forall a, b \in \mathbb{Z}$, $11|(2+a) \wedge 11|(35-b) \implies 11|(a+b)$.

Proof. Since 11 divides both $2+a$ and $35-b$, then, by Theorem 2.2, $2+a \equiv 35-b \pmod{11}$.

Adding b and subtracting 2 gives, $a+b \equiv 33 \equiv 0 \pmod{11}$. Thus, 11 divides $a+b$. □

Problem (2)**.** Use the Euclidean Algorithm to find

i) (1003, 456)
(456, 91)
(91, 1) = 1.

ii) (322, 148)
(148, 26)
(26, 18)
(18, 8) = 2.

iii) (5858, 1436)
(1436, 114)
(114, 68)
(68, 46) = 2.

Problem (3)**.** Express 1 as a linear combination of 1003 and 456.

From Problem 2, we have the remainders of 1003 / 456 and 456 / 91,

$$\begin{aligned} 91 &= 1 \cdot 1003 - 2 \cdot 456 \\ 1 &= 1 \cdot 456 - 5 \cdot 91. \end{aligned}$$

Then, we replace 91 in the second equation by its expression in terms of 1003 and 456,

$$\begin{aligned} 1 &= 1 \cdot 456 - 5(1 \cdot 1003 - 2 \cdot 456) \\ 1 &= 11 \cdot 456 - 5 \cdot 1003, \end{aligned}$$

which is our linear combination of 1 using 1003 and 456.

Problem (4)**.** Prove $\forall n \in \mathbb{Z}_{>0}$, $9|n \iff 9$ divides the sum of the digits of n.

Proof. ($\implies$) Note that, $\forall k \geq 0$, we can write $10^k = 1 + \sum_{j=1}^{k-1} 9(10^j)$.

Clearly, 9 divides the second term, so $10^k \equiv 1 + 0 = 1 \pmod 9$. So,

$$\forall k \geq 0,\ 10^k \equiv 1 \pmod 9. \tag{*}$$

Let $n = \sum_{j=0}^{k} 10^j a_j$ represent the decomposition of each digit a_j of n into powers of ten.

By (*) and Theorem 2.6, $n \equiv \sum_{j=0}^{k} a_j \pmod 9$.

But $9|n \implies n \equiv 0 \pmod 9$ by assumption, So $9|\sum_{j=0}^{k} a_j$ as well.

Thus, the sum of the digits a_j of n is divisible by 9 when n itself is divisible by 9.

($\impliedby$) Follows directly from reversing the proof, multiplying each digit a_j by 10^j. □

Problem (5)**.** Prove $\forall n \in \mathbb{Z}_{>0}$, $\frac{12n+1}{30n+2}$ cannot be reduced.

Proof. We will show that the greatest common divisor of the numerator and the denominator is one, indicating that the fraction is already in simplest form.

$$\begin{aligned} &(30n+2, 12n+1) \\ =&(12n+1, 6n) \\ =&(6n, 1) = 1. \end{aligned}$$

So, the fraction $\frac{12n+1}{30n+2}$ is already in simplest form. □

Problem (6)**.** Find the greatest common divisor of $(2^{100} - 1, 2^{120} - 1)$.

$(2^{100} - 1, 2^{120} - 1) = 2^{(120,100)} - 1 = 2^{10} - 1$.

Problem (7)**.** Prove $\forall a, b, c \in \mathbb{Z}_{>0}$, $c^2 = ab$, $(a, b) = 1 \implies a, b$ are perfect squares.

Proof. We wish to show that all primes factors of a and b must have even powers, this implies that a and b are themselves perfect squares.

Let the prime factorization of a and b be given respectively by

$$\prod_{i=1}^{k} p_i^{\alpha_i} \text{ and } \prod_{j=1}^{m} q_j^{\beta_j}.$$

So, by the commutativity of multiplication,

$$ab = \prod_{i=1}^{k}\prod_{j=1}^{m} p_i^{\alpha_i} q_j^{\beta_j}.$$

Since $c^2 = ab$, then the prime factorization of ab must have only even exponents.

So, whenever $p_i = q_j$ for some i, j, then $\alpha_i + \beta_j$ must be even.

But, $(a, b) = 1 \implies a, b$ share no common factors.

So, we will never have $p_i = q_j$ for any i, j.

So, $\forall i, j$, α_i and β_j must be even already.

Since all exponents of the prime factors of a and b are even, then a and b must be perfect squares. $\square$

Problem (8)**.** Prove for p prime, $1 \leq k < p$, $p|\binom{p}{k}$, $\quad \binom{p}{k}\frac{p!}{k!(p-k)!}$.

Proof. Note that, for $1 \leq k < p$, all factors of $k!(p-k)!$ will be less than p. So $(p, k!(p-k)!) = 1$.

Hence, $\frac{p!}{k!(p-k)!}$ will have one factor of p in the numerator, allowing us to write,

$$\binom{p}{k} = p\left(\frac{(p-1)!}{k!(p-k)!}\right).$$

Thus, $p|\binom{p}{k}$ by Corollary 1.6. $\square$

Problem (9)**.** Prove there are infinitely many primes.

Proof. For a contraction, assume that there are k finitely many primes $p_1, \ldots, p_k$.

Let $n = 1 + \prod_{i_1}^{k} p_i$. Since the right term of n has a factor of each prime, then $\forall i \in [1, k]$,

$$n \equiv 1 \pmod{p_i}.$$

Thus, n is not divisible by any of the primes. So, n must be a prime itself or have a prime factor not included in the finitely many k primes.

Since we have found a prime that is not in our original finite list, then our assumption must be false.

Therefore, there must be infinitely many primes. □

Problem (10). a) Show $\forall n \in \mathbb{Z}_{>0}$, $10^n \equiv 1 \pmod 9$.

b) Prove that every positive integer is congruent to the sum of its digits mod 9

Proof of a. See Problem 4. □

Proof of b. We can use the same expansion of n by powers of ten as in Problem 4 without the condition that the original n is divisible by 9. In such a case, we are still left with $n = a_0 10^0 + \cdots + a_k 10^k \equiv a_0 + \cdots + a_k \pmod 9$ by part a. □

Problem (11). Write the addition and multiplication tables for $\mathbb{Z}_4$ and $\mathbb{Z}_7$.

$\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Problem (12)**.** Solve the following for x:

a) $x^2 + x = [0]$ in $\mathbb{Z}_5$

b) $x^2 + x = [0]$ in $\mathbb{Z}_6$

c) Prove for p prime, the only solutions of $x^2 + x = [0]$ in $\mathbb{Z}_p$ are $[0]$ and $[p-1]$.

Proof of (a). By part (c), $x = [0], [4]$. □

Proof of b. By factoring, we have that

$$x(x+1) \equiv 0 \pmod 6.$$

First, we have $x = [0]$.

Then, we have the canonical representation factors of 6 which are congruent to zero: 1,6, 2,3, and 3,4.

So, $2(2+1) \equiv 0 \pmod 6 \implies x = [2]$ and $3(3+1) \equiv 0 \pmod 6 \implies x = [3]$

However, 1 and 6 are not consecutive integers, so they do not satisfy the equation.

Thus, $x = [0], [2], [3]$. □

Proof of c. By factoring, we have that

$$x(x+1) \equiv 0 \pmod p.$$

By Theorem 1.5, $x \equiv 0 \pmod p$ or $x + 1 \equiv 0 \pmod p$.

So, $x = [0]$ or $x \equiv -1 \equiv p - 1 \pmod p$.

Thus, $x = [0], [p-1]$ are the solutions to the equation where p is prime □