Math 402 Homework 2

Alexandre Lipson

January 22, 2025

Problem (1). a) Prove $66|43^{101} + 23^{101}$.

b) Prove $\forall n \in \mathbb{Z}_{\geq 0}$, $133|11^{n+2} + 12^{2n+1}$.

Proof of a. We will check the divisibility of the prime factors of 66: 2,3,11 separately.

By Theorem 2.3, the equivalence of congruence classes, working in $\mathbb{Z}_2$, $23 \equiv 43 \equiv 1 \implies 23^{101} \equiv 43^{101} \equiv 1$. So $43^{101} + 23^{101} \equiv 1 + 1 = 0 \implies 2|43^{101} + 23^{101}$.

Similarly, in $\mathbb{Z}_3$, $23 \equiv 2$ and $43 \equiv 2$.

Note that $2^{101} \equiv 2^{2\cdot 50+1} \equiv 4^{50} \cdot 2 \equiv 1^{50} * 2 = 2$ in $\mathbb{Z}_3$.

Then, $23^{101} \equiv 2^{101} \equiv 2$ and $43^{101} \equiv 1^{101} = 1$.

So, $43^{101} + 23^{101} \equiv 1 + 2 \equiv 0 \implies 3|43^{101} + 23^{101}$.

Again, but with $\mathbb{Z}_{11}$, $23 \equiv 1$ and $43 \equiv -1$.

So $23^{101} \equiv 1^1 01 = 1$ and $43^{101} \equiv (-1)^{101} = -1 \implies 43^{101} + 23^{101} \equiv 1 - 1 = 0 \implies 11|43^{101} + 23^{101}$.

Since 2,3,11 each divide $43^{101} + 23^{101}$, then their product 66 must as well. □

Proof of b. We will check the divisibility of the prime factors of 133, 7 and 19.

First, in $\mathbb{Z}_7$, $11 \equiv 4$ and $12 \equiv 5 \implies 11^{n+2} + 12^{2n+1} \equiv 4^{n+2} + 5^{2n+1}$.

The powers of 4 have a period of 3 in $\mathbb{Z}_7$, so 4^{n+2} will depend on $n + 2 \mod 3$.

The powers of 5 have a period of 6 in $\mathbb{Z}_7$, so 5^{2n+1} will depend on $2n + 1 \mod 6$.

We will combine $4^{n+2} + 5^{2n+1}$ for all unique values of each of the powers of 4 and 5 produced by

choices of n and check divisibility by 7.

n	4^{n+2}	5^{2n+1}	$4^{n+2}+5^{2n+1}$
0	2	5	0
1	1	6	0
2	4	3	0

.

Next, for $\mathbb{Z}_{19}$, the powers of 11 have a period of 3 and the powers of 12 have a period of 6.

Proceeding as above,

n	11^{n+2}	12^{2n+1}	$11^{n+2}+12^{2n+1}$
0	7	12	0
1	1	-1	0
2	11	8	0

.

Since both 7 and 19 divide $11^{n+2}+12^{2n+1}$, then so does their product 133. □

Problem (2)**.** Find all the units of

a) $\mathbb{Z}_7$ Since 7 is prime, all nonzero classes are units: $[1],\dots,[6]$.

b) $\mathbb{Z}_8$. Since 1,3,5,7 are coprime to 8, then their classes from the units of $\mathbb{Z}_8$.

c) $\mathbb{Z}_9$. Since $1,2,4,5,7,8$ are coprime to 9, then their classes form the units of $\mathbb{Z}_9$.

d) $\mathbb{Z}_{10}$. Since $1,3,7$ are coprime to 10, then their classes form the units of $\mathbb{Z}_{10}$.

Problem (3)**.** a) Prove that $[a]$ unit in $\mathbb{Z}_n \implies [a]$ is not a zero divisor.

b) Prove that $[a]$ zero divisor in $\mathbb{Z}_n \implies [a]$ is not a unit.

Proof of a. For a contradiction, suppose that $[a]$ is both a unit and a zero divisor;
$\exists x,y\in\mathbb{Z}_n,\ x,y\neq 0\ :\ ax=1,\ ay=0$.

Then,

$$\begin{aligned} & ax=ax+0=ax+ay=a(x+y)\\ \implies & a(x+y)=ax\\ \implies & x+y=x\\ \implies & y=0, \end{aligned}$$

which is a contradiction with the assumption that $ay=0$ had a nonzero solution. □

Proof of b. Follows from the contrapositive of (a). □

Problem (4)**.** Solve the following using exercise Hungerford 2.3.13.

a) $15x = 9$ in $\mathbb{Z}_{18}$.

b) $25x = 10$ in $\mathbb{Z}_{65}$.

Proof of a. We have that $a = 15$, $b = 9$, $n = 18$. Then, $(a, n) = (15, 18) = 3 = d$; we check that $3|9 \implies d|b$. Next,

$$a = da' \implies 15 = 3 \cdot 5 \implies 5 = a'$$
$$b = db' \implies 9 = 3 \cdot 3 \implies 3 = b'.$$

By Theorem 1.8, $(15, 18) = 3$ affords a linear combination such that $\exists u, v$ where

$$15u + 18v = 3 \implies u = -1,\ v = 1.$$

Thus, by exercise (13), the solutions are [-3],[-3+18],[-3+36].

Simplifying these classes into their canonical representations gives the single solution to the equation, [15].

Therefore $x = 15$ is a solution to $15x = 9$ in $\mathbb{Z}_{18}$. □

Proof of b. We have $(25, 65) = 5$, so $a = 25$, $b = 10$, $d = 5$, $n = 65$.

Then, the linear combination $25u + 65v = 5 \implies u = -5$, $v = 2$.

Thus, by (13), the solutions are [-10],[-10+65],[-10+130],[-10+195],[-10+260].

The canonical representation of these classes is [55].

Therefore $x = 55$ is a solution to the $25x = 10$ in $\mathbb{Z}_{65}$. □

Problem (5)**.** Prove that the product of units in $\mathbb{Z}_n$ is also a unit.

Proof. Let a, b be units in $\mathbb{Z}_n$. Let $c = ab$.

Since a, b are units, then $\exists a^{-1}, b^{-1} \in \mathbb{Z}_n \ : \ a \cdot a^{-1} = 1,\ b \cdot b^{-1} = 1$.

We wish to show that $\exists c^{-1} \ : \ c \cdot c^{-1} = 1$.

Consider the following,

$$c \cdot (a^{-1} \cdot b^{-1}) = (a \cdot b) \cdot (a^{-1} \cdot b^{-1}).$$

By the commutativity and associativity of multiplication in $\mathbb{Z}_n$, we have that

$$(a \cdot b) \cdot (a^{-1} \cdot b^{-1}) = (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) = 1 \cdot 1 = 1.$$

Therefore $\exists c^{-1} = (a^{-1} \cdot b^{-1}) \in \mathbb{Z}_n$.

Since c has a multiplicative inverse in $\mathbb{Z}_n$, then it is a unit. □

Problem (6)**.** Find and prove the condition for when $a \neq 0, ac = ab \implies c = b$ holds in $\mathbb{Z}_n$.

Proposition. This property holds where $\mathbb{Z}_n$ is an integral domain by Theorem 3.7. $\mathbb{Z}_n$ is an integral domain when n is prime.

Proof. $ac = ab \implies a(b-c) = 0$. Since $\mathbb{Z}_n$ is an integral domain, $a \neq 0 \implies b - c = 0$.

Otherwise, a would be a zero divisor, contradicting the integral domain condition.

Therefore, $b = c$. □

Problem (7)**.** Let p, q be distinct primes. Show $\varphi(pq) = (p-1)(q-1)$ where φ is Euler's totient function.

Proof. $\varphi(pq)$ gives the numbers in $I = [1, pq]$ which are coprime to pq. These numbers are not divisible by p or q.

We will count the numbers in I which are divisible by p or q and subtract the count from the total pq numbers.

The numbers in I divisible by p are $p, 2p, \ldots, (q-1)p$; there are $q-1$ such numbers.

The numbers in I divisible by q are $q, 2q, \ldots, (p-1)q$; there are $p-1$ such numbers.

The number in I divisible by both p and q is pq; there is one such number.

So, there are $(q-1) + (p-1) + 1 = p + q - 1$ numbers in I divisible by p or q.

Then, the total numbers in I not divisible by p or q is

$$pq - (p + q - 1) = pq - p - q + 1 = (p-1)(q-1).$$

Thus, $\varphi(pq) = (p-1)(q-1)$. □

Problem (8)**.** Prove $\forall n \in \mathbb{Z}_{\geq 0}$, $\forall a, b \in \mathbb{Z}$, $10^{3n+1} \neq a^3 + b^3$.

Proof. First, we will consider cubes in $\mathbb{Z}_7$.

$$0^3 \equiv 0$$
$$1^3 \equiv 1$$
$$2^3 = 8 \equiv 1$$
$$3^3 = 27 \equiv 6$$
$$4^3 = 64 \equiv 1$$
$$5^3 = 125 \equiv 6$$
$$6^3 = 216 \equiv 6$$

So, the sums of two cubes in $\mathbb{Z}_7$ is any combinations of 0,1,6.

$$0 + 0 \equiv 0$$
$$0 + 1 \equiv 1$$
$$0 + 6 \equiv 6$$
$$1 + 1 \equiv 2$$
$$1 + 6 \equiv 0$$
$$6 + 6 \equiv 5$$

Thus, the possible values of $a^3 + b^3$ in $\mathbb{Z}_7$ are 0,1,2,5,6. Note that 3 and 4 are not possible values.

Now, we will check the values of 10^{3n+1} in $\mathbb{Z}_7$. First, $10 \equiv 3 \implies 10^{3n+1} \equiv 3^{3n+1}$.

We will now calculate the powers of 3 in $\mathbb{Z}_7$.

$$3^0 \equiv 1$$
$$3^1 \equiv 3$$
$$3^2 \equiv 2$$
$$3^3 \equiv 6$$
$$3^4 \equiv 18 \equiv 4$$
$$3^5 \equiv 12 \equiv 5$$
$$3^6 \equiv 15 \equiv 1$$

So, powers of 3 in $\mathbb{Z}_7$ have a period of 6. Since $3n + 1 \mod 6 \equiv 1, 4$, then

$$3^{3n+1} \equiv 3^{3n+1 \mod 6} \equiv 3^1, 3^4 \equiv 3, 4.$$

So, $10^{3n+1} \equiv 3, 4$ in $\mathbb{Z}_7$.

But, the possible values of $a^3 + b^3$ in $\mathbb{Z}_7$ were 0,1,2,5,6, which do not contain the possible values of 10^{3n+1}, which were 3 and 4.

So, we have shown that, since this equality cannot hold in $\mathbb{Z}_7$, it cannot hold in $\mathbb{Z}$. □

Problem (9)**.** Describe the ring axiom not satisfied by following subsets of $\mathbb{Z}$.

a) All odd integers and zero.

This set S does not satisfy closure; $1, 3 \in S$ but $1 + 3 = 4 \notin S$.

b) All nonnegative integers.

This set S does not have additive inverses; e.g., there is no solution to $1 + x = 0$.

Problem (10)**.** Define multiplication in $\mathbb{Z}$ by $\forall a, b \in \mathbb{Z}$, $ab = 0$. Show that, with ordinary addition and the new multiplication, $\mathbb{Z}$ is a commutative ring.

Proof. Since we are modifying the multiplication operation, we need to ensure that closure and associativity for multiplication and distributivity are maintained.

Note that the multiplication operation maps all pairs of numbers in $\mathbb{Z}$ to $0 \in \mathbb{Z}$, so the new multiplication operation is closed.

For associativity, $a(bc) = a \cdot 0 = 0 = 0 \cdot c = (ab)c$, so multiplication is associative.

For distributivity, since $b+c \in \mathbb{Z}$ by the closure of addition already satisfied in $\mathbb{Z}$, then $a(b+c) = 0$ by the definition of the new multiplication operation.

But, $a(b + c) = ab + bc = 0 + 0 = 0$, so the new multiplication satisfies distributivity.

Since all axioms are maintained, $\mathbb{Z}$ is still a ring with the new multiplication operation.

Since $\forall a, b \in \mathbb{Z}$, $ab = 0 = ba$, then $\mathbb{Z}$ with the new multiplication operation is also a commutative ring. □