2015-09-14 Problems

Introduction to Number Theory

1. Let $x, y \in \mathbb{Z}$ and $m \in \mathbb{N}$. We say that x and y are congruent modulo m, if the diffference $x - y$ is divisible by m. We write

$$x \equiv y \pmod{m}.$$

Note that $x \equiv y \pmod{m}$ if and only if $x - y \in m\mathbb{Z}$. Show that the relation "$x \equiv y \pmod{m}$", gives an equivalence relation, say $\sim_m$, on $\mathbb{Z}$. That is, show that

- $a \sim_m a$,
- $a \sim_m b$ implies $b \sim_m a$, and
- $a \sim_m b$ and $b \sim_m c$ imply $a \sim_m c$.

2. Prove the following properties:
2.1. $a \equiv a' (\bmod m) \Rightarrow a + c \equiv a' + c (\bmod m)$ for any $c \in \mathbb{Z}$.
2.2. $a \equiv a' (\bmod m) \Rightarrow ac \equiv a'c (\bmod m)$
2.3. $a \equiv a', b \equiv b' (\bmod m) \Rightarrow ab \equiv a'b', a + b \equiv a' + b' (\bmod m)$.
2.4. Give a counter-example to $a \equiv a' (\bmod m) \Rightarrow a/c \equiv a'/c (\bmod m)$.
2.5. Show that $a \equiv a' (\bmod m_1)$ and $a \equiv a' (\bmod m_2) \Rightarrow a \equiv a' (\bmod lcm(m_1, m_2))$.
2.5.1. Give a counter-example to $a \equiv a' (\bmod m_1)$ and $a \equiv a' (\bmod m_2) \Rightarrow a \equiv a' (\bmod m_1 m_2)$.
2.6. Show that $ac \equiv a'c (\bmod m) \Rightarrow a \equiv a' (\bmod m/gcd(m, c))$.
2.6.1. Give a counter-example to $ac \equiv a'c (\bmod m) \Rightarrow a \equiv a' (\bmod m)$.

3. The set of equivalence classes in the problem above will be denoted $\mathbb{Z}/m\mathbb{Z}$. We write $\overline{a}$ or $\overline{a}_m$ for the element in $\mathbb{Z}/m\mathbb{Z}$ represented by the element $a \in \mathbb{Z}$.
Show that there is a 'natural' structure of ring on $\mathbb{Z}/m\mathbb{Z}$.

4.1. Let R be a (commutative unital) ring. An element $r \in R$ is said to be invertible if there exists an element $u \in R$ such that $ru = 1$. Show that the set of invertible elements $R^\times$ form an abelian group under multiplication of R.
4.2. Deleted due to an error.

5.1 Show that an element $c \in \mathbb{Z}/m\mathbb{Z}$ is invertible (i.e., there exists an element d such that $cd \equiv 1(m)$) if and only if $gcd(c, m) = 1$.
The set of invertible elements is denoted $(\mathbb{Z}/m\mathbb{Z})^\times$.
5.2. List the invertible elements in $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/25\mathbb{Z}$, and $\mathbb{Z}/125\mathbb{Z}$. What is the cardinality of $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/25\mathbb{Z})^\times$, and $(\mathbb{Z}/125\mathbb{Z})^\times$ respectively?

6.1. (Euler's function) Let $\varphi(n)$ denote the cardinality of $(\mathbb{Z}/n\mathbb{Z})^\times$. (We set $\varphi(1) = 1$.)
6.2. Find all integers n such that $\varphi(n) = 2, 3, 4, 5, 6, 7$.
6.3. Show that $\sum_{d|n} \varphi(d) = n$.
6.4. Let $n \in \mathbb{N}$. For $a \in \mathbb{Z}$ such that $gcd(a, n) = 1$, set f to be the smallest positive integer such that $a^f \equiv 1 (\bmod n)$. Show that $f | \varphi(n)$.

7. Let $m, n \in \mathbb{N}$. Determine the kernel of the ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, that sends $1 \in \mathbb{Z}$ to $(\bar{1}, \bar{1})$.

8.1. Show that $10^{2n+1} + 1$ is divisible by 11.
8.2 Show that $7^{20} - 1$ is divisible by 25.

9. Show that n is prime if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field.

10.1. (Wilson's theorem) Show that if p is prime, then $(p-1)! \equiv -1 (\bmod p)$. Hint: Note that $(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \dots, \overline{p-1}\}$ is a group so there exists a unique inverse to each of the elements.
10.2. Show that the converse holds. (That is, if $(p-1)! \equiv -1 (\bmod p)$, then p is prime.)

11. Let p be prime. Recall that a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$ is called a primitive root modulo p. Give an example of a primitive root modulo p for $p = 3, 5, 7, 11, 13, 17$.

12.1. Show that $2^{1093} - 2$ is divisible by 1093^2. (may use a calculator)
12.2. Show that $2^{3511} - 2$ is divisible by 3511^2. (may use a calculator)

13. Let p be an odd prime. Let $e \in \mathbb{N}$. Show $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is a cyclic group. Hint: Show that $\overline{p+1} \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ is of order p^{e-1}. Show $(\mathbb{Z}/p^e\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^e\mathbb{Z}$. Use $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

14.1. Let p be an odd prime. Show that the order f of $\overline{10} \in \mathbb{Z}/p\mathbb{Z}$ is a divisor of $p-1$. Show that the decimal expansion of $\frac{1}{p}$ is a repeating decimal of period f.
14.2. Verify the claim directly when $p = 7, 11$, or 13.

15.1. Suppose p and $q := 2p+1$ are primes and $p \equiv 1 (\bmod 4)$. Show that 2 is a primitive root modulo q.
15.2. Suppose p and $q := 4p+1$ are odd primes. Show that 2 is a primitive root modulo q.

16. Show that there exist infinitely many primes p such that $p \equiv 1 (\bmod 4)$.

Milnor's K-groups

Let k be a field. For $n \in \mathbb{N}$, we define the n-th Milnor K-group of k to be

$$K_n^M(k) = (k^\times \otimes_\mathbb{Z} \cdots \otimes_\mathbb{Z} k^\times)/I_n$$

where I_n is the subgroup generated by elements of the form $a_1 \otimes \cdots \otimes a_n$ with $a_i + a_j = 1$ for some $i \neq j$. The element of $K_n^M(k)$ represented by the element $a_1 \otimes \cdots \otimes a_n \in k^\times \otimes_\mathbb{Z} \cdots \otimes_\mathbb{Z} k^\times$ is written $\{a_1, \dots, a_n\}$. We set $K_0^M(k) = \mathbb{Z}$. For $n = 1$, we have $K_1^M(k) = k^\times$

MK1. Show that $\{a_1, \dots, a_d\} = 0$ if $a_i + a_j = 0$ for some $i \neq j$.

MK2. Show $\{\dots, a_i, \dots, a_j, \dots\} = -\{\dots, a_j, \dots, a_i, \dots\}$ (exchange the i-th and the j-th entries).

MK3. If $a + b \neq 0$, show $\{a, b\} = \{a + b, -a^{-1}b\}$.

MK4. Show $\{a_1, \dots, a_n\} = 0$ if $a_1 + \cdots + a_n = 0$ or if $a_1 + \cdots + a_n = 1$.

MK5.1. Show that $K_2^M(\mathbb{Z}/5\mathbb{Z}) = 0$.

MK5.2. Let p be a prime number. Let k be a finite field of p elements. Show that $K_n^M(k) = 0$ for $n \geq 2$.

MK5.3. Show that $K_n^M(k) = 0$ for $n \geq 2$ holds for any finite field k.