Finite Fields

Division in Modular Arithmetic

Let p be a prime everywhere in the text below. In $\mathbb{Z}_p$ -arithmetic we write just $a=b$ instead of $a \equiv_p b$

Definition. For $n \neq 0$ a fraction m/n means the only $q \in \mathbb{Z}_p$ such that $qn=m$. The *inverse* of n is $1/n=n^{-1}$

1. Find 2/7 mod 11, 4/18 mod 19, 11/5 mod 101.

2. Prove that **a)** $m/n=m\cdot 1/n$ **b)** $(a+b)/n=a/n+b/n$ **c)** $m/n\cdot p/q=mp/nq$
d) $m/n+p/q=(mq+np)/nq$

3. (*Linear representation of gcd*) Prove that if integers a and b are coprime, then there exist integers u and v such that gcd(a, b)=ua+vb.

Advice. A practical way to find coefficients u and v is to use Euclidian algorithm to find gcd(a, b). The inverse of n is the coefficient u in the representation 1=gcd(n, p)=un+vp.

4. a) Find the sum 1/1+1/2+ …+1/(p–1) in $\mathbb{Z}_p$

b) The sum of real fractions 1/1, 1/2, …, 1/(p–1) is written as an uncancelled fraction. Prove that if p>2 then the numerator is divisible by p.

c) The sum of real fractions $1/1^2$, $1/2^2$, …, $1/(p-1)^2$ is written as an uncancelled fraction. Prove that if p>3 then the numerator is divisible by p.

5. a) Show that $\binom{p}{k}=\frac{p!}{k!\cdot(p-k)!}$ is divisible by p for k=1, 2, …, p-1.

b) Prove that $(a+b)^p=a^p+b^p \quad \forall\, a, b \in \mathbb{Z}_p$

c) Deduce a new proof of Fermat's little theorem from (b).

RO. a) A sultan decides to give 100 of his sages a test. He has the sages stand in line, one behind the other, so that the last person in line can see everyone else. The sultan puts either a black or a white hat on each sage. The sages can only see the colors of the hats on all the people in front of them. Then, in any order they want, each sage guesses the color of the hat on his own head. Each hears all previously made guesses, but other than that, the sages cannot speak. Each person who guesses the color wrong will have his head chopped off. The ones who guess correctly go free. The rules of the test are given to them one day before the test, at which point they have a chance to agree on a strategy that will minimize the number of people who die during this test. Is there a strategy to save 99 of them for certain?
b) The same question for the test with red, blue and green hats.

Polynomials with coefficients in $\mathbb{Z}_p$

Definition. Fix a set **K** of coefficients, e.g., $K=\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_p, \mathbb{C}$. Let **K**[x] be the set of polynomials with coefficients in K.
Two polynomials of $\mathbf{Z}_p[x]$ are equal if their standard forms coincide (i.e. they have same degree and same coefficients).
6. a) Can every value of a nonzero polynomial of $\mathbf{Z}_p[x]$ be equal to 0?
b) Can a product of two nonzero polynomials of $\mathbf{Z}_p[x]$ be equal to 0?
7. a) Prove that $\mathbf{Z}[x]$ and $\mathbf{Z}_p[x]$ are closed under addition, subtraction and multiplication.
b) Is $\mathbf{Z}[x]$ closed under division with remainder if the leading coefficient of the divisor is 1?
c) Is $\mathbf{Z}_p[x]$ closed under division with remainder?
d) Is Bézout's theorem true for $\mathbf{Z}_p[x]$?
e) Can a polynomial of degree n of $\mathbf{Z}_p[x]$ have more then n roots ?

8 a) Prove the identity $x^{p-1}-1 = (x-1)(x-2)\ldots(x-(p-1))$ for $\mathbf{Z}_p[x]$.
b) Deduce a new proof of Wilson's theorem from (a).

9 a) Prove that $F(x)^p = F(x^p)$ for every $F \in \mathbb{Z}_p[x]$

b) Deduce from (a) that $p \mid \binom{p^n}{k} \quad \forall\ k \neq 0, p^n$

10*. How many of the coefficients of the polynomial $(x+1)^{100}$ are even?

Irreducible polynomials

Definition. A polynomial of **K**[x] is said to be *irreducible* over **K** if it does not split into the product of lesser degree polynomials of **K**[x].

11. The map $Rem_p : \mathbb{Z} \to \mathbb{Z}_p$ is also the map $Rem_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ (we just replace the coefficients with its remainders modulo p). Prove that the map preserve polynomial arithmetic.

12. a) Show that if $F \in \mathbb{Z}[x]$ is reducible over $\mathbb{Z}$ and $Rem_p(F) \neq 0$ then $Rem_p(F)$ is reducible over $\mathbb{Z}_p$.

b) $Rem_p(F)$ is reducible over $\mathbb{Z}_p$. Does this imply F is reducible over $\mathbb{Z}$?

Theorem 13. (*Eisenstein's criterion*) For a polynomial with integer coefficients, let all the coefficients, except for that of the leading term, be divisible by a prime p, and the constant term be not divisible by p^2 . Then the polynomial is irreducible over $\mathbb{Z}$.

14. Is the polynomial $x^n - 40! x^k + 30!$ reducible over $\mathbb{Z}$ for some k and n?

15. Prove that the equation $x^3 + 15x^2 - 24x + 21$ has no rational roots.

16. Determine GCD of $(x-1)^{103}+1$ and $(x+1)^{101}-1$ over $\mathbb{Z}$.

Extra problems

FF1. Prove that for each prime p there is a polynomial of $\mathbf{Z}_p[x]$ without roots and
a) of degree 2; **b)** of every degree greater then $p - 1$.

FF2. $P \in \mathbb{Z}[x], deg(P) < p-1$ and $p \mid P(k) \quad \forall\ k \in \mathbb{Z}$. Prove that all coefficients of P are divisible by p.

FF3. Prove that for each prime p the polynomial $x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible over $\mathbb{Z}$. (Hint. For $P \in \mathbb{Z}[x]$ and $m \in \mathbb{Z}$ polynomials $P(x)$ and $P(x+m)$ either are both reducible or both irreducible over $\mathbb{Z}$)

FF4. Let $a_1, a_2, \ldots, a_n$ be distinct integers. Prove that the polynomial $P(x) = (x-a_1)(x-a_2)\ldots(x-a_n) - 1$ is irreducible over .