Finite Fields Z_p

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) $m/n+p/q=(mq+np)/nq$

Definition. We see $\mathbf{Z}_p$ has division as well as addition and multiplication, so $\mathbf{Z}_p$ is a field, as good as $\mathbb{Q},\mathbb{R},\mathbb{C}$. So we can consider polynomials $\mathbf{Z}_p[x]$, vector space $\mathbb{Z}_p^n$ and matrices with entries from $\mathbf{Z}_p$.

3. Find the sum $1/1+1/2+\ldots+1/(p-1)$ in $\mathbb{Z}_p$

Definition. Two polynomials of $\mathbf{Z}_p[x]$ are equal if their standard forms coincide (i.e. they have same degree and same coefficients).

4. a) How many elements consists $\mathbb{Z}_p^n$ of?
b) How many polynomials of grade 3 are there in $\mathbf{Z}_p[x]$?
5. 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?
6. 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 ?

7. Prove the identity $x^{p-1}-1=(x-1)(x-2)\ldots(x-(p-1))$ for $\mathbf{Z}_p[x]$.

Projection from Z to Z_p

Definition. $Rem_p:\mathbb{Z}\to\mathbb{Z}_p$ Just replaces integers with its remainders modulo p. It can be extended to vectors, matrices and polynomials, replacing integer entries and coefficients with their remainders modulo p.
Obviously, Rem_p preserves addition, multiplication, substitution in polynomial, determinant, transposition of matrices.To be short, let us fix a prime p and denote $Rem_p(A)=A'$ for any object A be integer, vector, polynomial or matrix.

8. Let $m\in\mathbb{Z},P(x)\in\mathbb{Z}[x],\vec{u},\vec{v},\ldots,\vec{w}\in\mathbb{Z}^n$, M be a matrix with integer entries. Prove that **a)** $deg(P')\leq deg(P)$ **b)** If $P'(m')=0$ then $p|P(m)$; **c)** If $\vec{u}',\vec{v}',\ldots,\vec{w}'$ are lineary independent then $\vec{u},\vec{v},\ldots,\vec{w}$ are also lineary independent; **d)** $rank(M')\leq rank(M)$.

9. A square matrix M with integer entries has odd entries on the main diagonal and even entries above the diagonal. Prove that $det(M)\neq 0$.

10. The sum of real fractions 1/1, 1/2, …, $1/(p-1)$ is written as an unreduced fraction. Using problem 3, prove that if $p>2$ then the numerator is divisible by p.

11. Deduce from problem 7 a new proof of Wilson's theorem from (a).

Credit problems

ZP1. The sum of real fractions $1/1^2$, $1/2^2$, …, $1/(p-1)^2$ is written as an uncancelled fraction. Prove that if prime $p>3$ then the numerator is divisible by p.
ZP2. Prove that for each prime p there is a polynomial in $\mathbf{Z}_p[x]$ without roots and
a) of degree 2; **b)** of every degree greater then $p-1$.
ZP3. $P\in\mathbb{Z}[x], deg(P)<p-1$ and $p|P(k) \quad \forall k\in\mathbb{Z}$. Prove that all coefficients of P are divisible by p.
ZP4. How many coefficients of the polynomial $(x+1)^{100}$ are even?

www.ashap.info/Uroki/eng/NYUAD18/index.html