Discrete Mathematics

COMS 3203 – Fall 2017

http://www.cs.columbia.edu/~amoretti/3203

Homework # 4

Due Sunday, November 19th

This problem set includes a few extra questions that draw on concepts outside of the scope of this course. In particular the last few questions denoted $(\star)$ are nontrivial. You do not need to submit these questions but you may be interested in exploring connections with other areas in mathematics. **Solve any seven problems for full marks**. You are encouraged to form study groups and discuss with your classmates, come to office hours and post on Piazza but the write up must be your own.

1. (Problem 7.33)

(!) 1500 soldiers arrive in training camp. A few soldiers desert the camp. The drill sergeants divide the remaining soldiers into groups of five and discover that there is one left over. When they divide them into groups of seven, there are three left over. When they divide them into groups of eleven, there are again three left over. Determine the number of deserters.

2. (Problem 7.46)

(!) A *cyclic shift* of a p-tuple x is a p-tuple obtained by adding a constant (modulo p) to the indices of the elements of x; shifting x by $p+i$ positions produces the same p-tuple as shifting x by i positions. For $a \in \mathbb{N}$, let R be the relation on $[a]^p$ (the set of p-tuples with entries in $\{1, \cdots, a\}$) defined by putting $(x, y) \in R$ if the p-tuple y can be obtained from x by a cyclic shift.

1. Prove that R is an equivalence relation on $[a]^p$.
2. Use (1.) and Lemma 7.27 to prove that p divides $a^p - a$ when p is prime. *Hint:* Partition a set of size $a^p - a$ into subsets of size p.
3. Use (2.) to prove Fermat's Little Theorem.

3. (Problem 7.47)

Let p be an odd prime. Prove that $2(p-3)! \equiv -1 \bmod p$. *Hint:* Use Wilson's Theorem, Theorem 7.44.

4. (Problem 7.50)

Prove that the polynomials of degree k with coefficients in $\mathbb{Z}_p$ form a group under addition modulo p.

5. Direct Product of Groups

Let's define the direct product of two groups, $\mathcal{G}$ and $\mathcal{H}$ by considering elements of $\mathcal{G} \times \mathcal{H}$ as ordered pairs (g, h) where $g \in \mathcal{G}$ and $h \in \mathcal{H}$. When $\mathcal{G}$ has n elements and $\mathcal{H}$ has n' elements, their product $\mathcal{G} \times \mathcal{H}$ has $n \cdot n'$ elements. We define the direct product using the operation of $\mathcal{G}$ denoted $\circ_{\mathcal{G}}$ and the operation of $\mathcal{H}$ denoted $\circ_{\mathcal{H}}$ applied component wise:

$$(g, h) \circ (g', h') = (g \circ_{\mathcal{G}} g', h \circ_{\mathcal{H}} h') \tag{1}$$

Prove that $\mathcal{G} \times \mathcal{H}$ is a group.

6. Bezout's Identity and Euclid's Algorithm

Suppose we are given a sequence of integers $n_1, \cdots, n_k$ whose GCD is equal to d (where $d = 1$). Bezout's identity states that there exists another sequence of integers $a_1, \cdots, a_k$ such that $a_1 n_1 + \cdots + a_k n_k = d$. Prove Bezout's identity and show that Euclid's algorithm can be used to find the co-prime GCD of the sequence (*Hint:* Euclid's algorithm can be used to prove Bezout's identity).

7. Modular Arithmetic

Let p, n be integers with $p|n$. Prove that, for any $x \in \mathbb{Z}$:

$$[(x \bmod n) \bmod p] = [x \bmod p] \tag{2}$$

Show that $[(x \bmod p) \bmod n] \neq [x \bmod n]$.

8. Chinese Remainder Theorem

Use the Chinese Remainder Theorem to compute 46^{51} mod 55 by hand.

9. Vandermonte Matrices, Polynomials and Fields

Vandermonte matrices are commonly used to represent polynomials and play an important role in applied mathematics for curve fitting and interpolation. Prove that the following statement is true in any field:

$$det \begin{bmatrix} x_1^0 & x_2^0 & x_3^0 & \dots & x_n^0 \\ x_1^1 & x_2^1 & x_3^1 & \dots & x_n^1 \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_n^2 \\ \vdots & \vdots & \dots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \dots & x_n^{n-1} \end{bmatrix} = det \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ x_1 & x_2 & x_3 & \dots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_n^2 \\ \vdots & \vdots & \dots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \dots & x_n^{n-1} \end{bmatrix} = \prod_{i<j} (x_j - x_i) \tag{3}$$

The product here is over all terms $x_j - x_i$ where $1 \leq i \leq j \leq n$. For example when $n = 3$ the product is defined $\prod_{i<j} (x_j - x_i) = (x_3 - x_1)(x_3 - x_2)(x_2 - x_1)$. *Hint*: Use induction, starting with the case $n = 2$ using the formula for the determinant of a 2×2 matrix.

10. Linear Algebra and Number Theory

($\star$) Suppose we are given two vectors, $\mathbf{x}, \mathbf{y} \in \mathbb{R}^k$, where $\|\mathbf{x}\| = \|\mathbf{y}\|$. We say that a complex square matrix $\mathbf{U} \in \mathbb{C}^k$ is unitary if it's product with its conjugate transpose $\mathbf{U}^\dagger\mathbf{U}$ returns the identity I.

1. Can you construct a unitary matrix $\mathbf{U}$ such that 1) $\mathbf{U}\mathbf{x} = \mathbf{y}$, 2) $\mathbf{U}$ is rational if $\mathbf{x}, \mathbf{y}$ are rational, and 3) the product $\mathbf{U}\mathbf{x}$ is computed in linear time? *Hint:* draw two vectors in $\mathbb{R}^2$ and define a distance between them. Take a plane through $\mathbf{x}$, $\mathbf{y}$ orthogonal to the segment that connects them and look at the reflection of that plane. Design a symmetric matrix using this and subtract it from the identity to form $\mathbf{U}$.

2. In class we saw Fermat's Last Theorem. We are interested in Pythagorean triples $a^n + b^n = c^n$ (Pythagorean tuples $a_1^2 + \cdots + a_n^2 = a_{n+1}^2$ also work) when $n = 2$. Take the equation, divide by c (or a_{n+1}) and consider the norm:
$$\left\| \frac{a}{c}, \frac{b}{c} \right\| = 1 \tag{4}$$
This can be used to show all solutions give rational points on the unit sphere. Between any two real points on the unit circle there exists a rational point.

3. Scale the matrix $\mathbf{U}$, take its first column and give an algorithm to generate solutions to the following equations of Pythagorean triples:
$$a^2 + b^2 = c^2 \tag{5}$$

11. Bezout's Identity and Polynomials

($\star$) Prove the general case of Bezout's identity $q_1p_1 + q_np_n = 1$. Start with a polynomial:

$$x^n - a_{n-1}x^{n-1} - \cdots - a_0 = R(x) \tag{6}$$

The set of all polynomials of degree at most $n-1$ belong to some field:

$$\{P(x) = \sum_{i=0}^{n-1} b_i x^i : b_i \in \mathcal{F}\} \tag{7}$$

For two polynomials p and r, we can write their product as $p \cdot q = [p \cdot q]_r$ to say that $p = q \cdot r + d$. Hint: if you can find d_1, d_2 such that $d_1p + d_2r = 1$, this implies that $[p \cdot q]_r = 1$ and that $GCD(p, r) = 1 \; \forall p \neq 0$, which means that the polynomial is irreducible.

12. Irreducible Polynomials and Finite Fields

($\star$) In this question we will work with fields mod p for some prime p, denoted $\mathcal{F}_p$. Consider a polynomial of degree n, p^n over this field where $v_i \in \{0, 1, \cdots, p-1\}$. Prove that for any finite field, there exists an irreducible polynomial of degree n. *Hint:* Start with the field $\mathcal{F}_p$ and build a matrix (call it $\mathbf{A}$), which is a shifted identity with coefficients of the irreducible polynomial in the last column. Make sure you have looked at question 9.