15-251 : Great Theoretical Ideas In Computer Science

Fall 2014

Assignment 7

Due: **Friday**, Oct. 24, 2014 11:59 PM

Name: _____

Andrew ID: _____

Question:	1	2	3	4	Total
Points:	25	25	25	25	100
Score:					

0. Warmup

(a) How many generators does $\mathbb{Z}_{pq}$ (under the + operation) have where p, q are primes?

(b) Let G be a group where every element (besides the identity) has order 2. Prove that G is abelian.

(c) Prove that there is a unique group up to isomorphism with 251 elements.

(d) Consider the "mattress" group K_4 with the following group table:

$\circ$	I	R	F	H
I	I	R	F	H
R	R	I	H	F
F	F	H	I	R
H	H	F	R	I

Write down all the *proper* subgroups of K_4.

(e) Let H be a proper subgroup of a finite group G. For an element $g \in G$, denote by gH the set $\{gh \mid h \in H\}$.

1. Let $g_1, g_2 \in G$. Prove that the sets g_1H and g_2H are equal if $g_1^{-1}g_2 \in H$ and disjoint otherwise.
2. Use the above to prove Lagrange's theorem, namely $|G|$ is divisible by $|H|$.

(f) Verify that the subset of complex numbers $\mathbb{Q}(i) = \{a+bi \mid a, b \in \mathbb{Q}\}$ where $i = \sqrt{-1}$ is a field under addition and multiplication as complex numbers. (Here, as usual, $\mathbb{Q}$ denotes the field of rationals.)

(g) Find a polynomial $f(X) \in \mathbb{F}_{13}[X]$ of degree at most 2 satisfying $f(0) = 1$, $f(1) = 0$, and $f(6) = 5$.

(h) Find the smallest positive integer n satisfying $n \equiv 1 \pmod 9$, $n \equiv 2 \pmod{10}$, and $n \equiv 7 \mod 11$.

(i) Prove that polynomials of degree at most 2 in $\mathbb{F}_2[x]$, with addition and multiplication modulo $(1 + x + x^3)$, form a finite field with 8 elements.

1. Product of two elements and 251 primes

(10) (a) Let A be a subset of a finite group G with $|A| > |G|/2$. Prove that every element of G can be written as the product of two elements of A. Is this also aways true when $|A| = |G|/2$?

Solution:

(15) (b) Prove that there are 15251 consecutive positive integers each of which is divisible by at least 251 distinct primes.

(You may use the existence of an infinite supply of prime numbers.)

Solution:

2. Cyclic prime fun

Let p be a prime number. Consider the group $\mathbb{Z}_p^*$ of integers $\{1, 2, \ldots, p-1\}$ under multiplication modulo p.

(8) (a) Let d be a divisor of $(p-1)$. Prove that there are *exactly* d elements a in $\mathbb{Z}_p^*$ that satisfy $a^d = 1$.

Hint: Use Fermat's little theorem and the polynomial factorization $X^{p-1} - 1 = (X^d - 1)(X^{d(k-1)} + X^{d(k-2)} + \cdots + X^d + 1)$ where $k = (p-1)/d$.

Solution:

(5) (b) Prove the following for any positive integer n

$$\sum_{d|n} \phi(d) = n$$

where $\phi(\cdot)$ is the Euler totient function and $d|n$ means that d divides n, so the sum is over all the divisors of n (including $1, n$).

Hint: Partition elements $a \in \{1, 2, \ldots, n\}$ based on $\gcd(a, n)$.

Solution:

(12) (c) Using the previous two parts, prove that the group $\mathbb{Z}_p^*$ is cyclic.

Solution:

3. Fun with polynomials

(10) (a) Consider the polynomial $P(X) = (X-1)(X-2)\cdots(X-250)(X-251)+1$. Prove that $P(X)$ is irreducible over the integers, i.e., one cannot write $P(X) = Q(X)R(X)$ for polynomials Q, R with integer coefficients unless either Q or R is a constant polynomial (equal to ± 1).

Hint: Suppose that $P(X) = Q(X)R(X)$ where degree of both Q and R is less than 251, and derive a contradiction.

Solution:

(15) (b) A polynomial $P(X)$ with integer coefficients will certainly satisfy $P(n) \in \mathbb{Z}$ for every $n \in \mathbb{Z}$. However, there also exist polynomials with non-integer coefficients that take integer values at all integer points. For example, the polynomials $\binom{X}{m}$ for $m \in \mathbb{N}$ defined by

$$\binom{X}{m} = \frac{X(X-1)(X-2)\cdots(X-m+1)}{m!} .$$

Prove that a degree d polynomial $P(X)$ with rational coefficients satisfies $P(n) \in \mathbb{Z}$ for every $n \in \mathbb{Z}$ *if and only if* it can be written in the form

$$P(X) = a_0 + a_1\binom{X}{1} + a_2\binom{X}{2} + \cdots + a_d\binom{X}{d} \tag{1}$$

for some integers a_j, $j = 0, 1, \ldots, d$.

Hint (for the 'only if' part): First argue that any degree d polynomial can be expressed in the form (1) with *real* coefficients a_j. Then show that the a_j's have to be integers.

Solution:

4. Groups catch errors

(8) (a) The ISBN (International Standard Book Number) is a system to identify books published worldwide. The ISBN of a book is usually found on the last cover page. The current standard (as of January 1, 2007) uses a 13-digit system, but for this problem let us work with the older 10-digit code where the first nine digits identify the book and the last digit is a *check digit* to detect mistakes in, say, typing or communicating ISBNs. An ISBN can thus be viewed as a sequence of 10 digits $x_1x_2\ldots x_{10}$ where for all $i = 1, 2, \ldots, 9$, x_i is one of the digits $0, 1, 2, \ldots, 9$ (the exact way these are assigned by publishers is not important to us here). The check digit x_{10} has 11 possible values $\{0, 1, 2, \ldots, 10\}$ (if the check digit happens to be a 10, it is denoted by the roman numeral X), determined by the following congruence:

$$1x_1 + 2x_2 + \cdots + 8x_8 + 9x_9 + 10x_{10} \equiv 0 \pmod{11} .$$

(i) Let $x_1x_2\cdots x_9x_{10}$ be the correct ISBN of a book. Suppose that, during the billing procedure, a single error has been made in entering the ISBN; i.e, in the i'th place for some i, y_i is printed instead of x_i where $x_i \neq y_i$. Prove that this error can be *detected*; formally, show that the resulting 10 digit sequence is not a valid ISBN.

(ii) Same as above, except now consider the error where two *unequal* digits x_i, x_j are swapped, that is an error of the form

$$x_1x_2\cdots\mathbf{x}_i\ x_{i+1}\cdots\mathbf{x}_j\ x_{j+1}\cdots x_9x_{10} \longrightarrow x_1x_2\cdots\mathbf{x}_j\ x_{i+1}\cdots\mathbf{x}_i\ x_{j+1}\cdots x_9x_{10}$$

where $x_i \neq x_j$.

Solution:

(5) (b) The above ISBN system was thus able to detect single symbol errors and transpositions (swaps) of an *arbitrary* pair of symbols. However, it will be nice to have a code over just the decimal system, without needing the roman numeral X.

Let us now see such a system, which is the basis of the bank routing numbers in the United States. The check digit scheme used on routing numbers uses a 9-digit number with position weightings of 3, 7, and 1. Specifically, the check equation for a number $x_1x_2\ldots x_9$ (where each $x_j \in \{0, 1, \ldots, 9\}$) is

$$3(x_1 + x_4 + x_7) + 7(x_2 + x_5 + x_8) + (x_3 + x_6 + x_9) \equiv 0 \pmod{10} .$$

It is easy to see, as with the ISBN system, that the above check rule is able to detect single errors.

Prove, however, that this system sometimes *fails* to detect *some* adjacent transpositions (a common form of error) where x_ix_{i+1} (with $x_i \neq x_{i+1}$) are swapped for some i, i.e., an error of the form

$$x_1\cdots x_{i-1}\underline{x_ix_{i+1}}x_{i+2}\cdots x_9 \longrightarrow x_1\cdots x_{i-1}\underline{x_{i+1}x_i}x_{i+2}\cdots x_9 . \qquad (2)$$

Solution:

(12) (c) Given the previous parts you are now losing sleep over constructing a decimal check digit system that can detect adjacent transpositions of the form (2). Fortunately, as a 15-251 student, you are familiar with basic group theory, and know a nice group with 10 elements, namely the dihedral group D_5 of symmetries of the regular pentagon.

Recall that D_5 has 10 elements $\{\mathrm{Id}, r_1, r_2, r_3, r_4, f_1, f_2, f_3, f_4, f_5\}$, where as in lecture, r_i denotes clockwide rotation by $(72i)^\circ$ degrees and f_j denotes reflection about its axis through j.

(i) Consider the bijection $\sigma : D_5 \to \{0, 1, 2, \ldots, 9\}$ where $\sigma(\mathrm{Id}) = 0$, $\sigma(r_i) = i$ for $i = 1, 2, 3, 4$ and $\sigma(f_j) = 4 + j$ for $1 \leq j \leq 5$.
Is this an isomorphism between D_5 and $\mathbb{Z}_{10}$ (under addition modulo 10)? Justify your answer (in at most one sentence).

(ii) Let $\{a_0, a_1, \ldots, a_9\}$ be an arbitrary enumeration of elements of D_5.

It turns out that one can construct a "magic" bijection $T : D_5 \to D_5$ such that for *all* $i \neq j$, then $a_i \cdot T(a_j) \neq T(a_i) \cdot a_j$ (here $i, j \in \{0, 1, \ldots, 9\}$, and $\cdot$ denotes the group operation in D_5).

You do *not* have to construct a magic T as claimed above; however, can you tell your 251 TAs how to use T to construct a 10-digit decimal check digit system that can detect single digit errors *and* **all adjacent transpositions**?

In other words, specify a check rule using T for sequences $(x_1, x_2, \ldots, x_{10}) \in \{0, 1, \ldots, 9\}^{10}$ such that starting with a valid sequence satisfying the check rule, swapping x_i and x_{i+1} for $x_i \neq x_{i+1}$ as in (2) leads to a violation of the check rule.

Solution: