Mathematics 360 **Homework (due Nov 21)** A. Hulpke

53) Let $p = 109 = 2^2 3^3 + 1$. Then 6 is a primitive root modulo p. Using the Pohlig Hellman method and Hensel lifting, determine e such that $6^e \equiv 103 \pmod{p}$.

54) Let $p = 997$ (which is prime).
a) Find e such that $(a^{71})^e \equiv a \pmod{p}$. (Hint: $a^{996} \equiv 1$, so you want $a^{71e+996f} \equiv a^1 \pmod{p}$)
b) We note that $\mathrm{OrderMod}_p(320) = 332 = \frac{p-1}{3}$. How many $1 \le a < p$ exist such that $a^3 \equiv 320 \pmod{p}$? Explain!
c) Determine all a such that $a^3 \equiv 320 \pmod{p}$. (**Hint:** 7 is a primitive root modulo p and $7^{675} \equiv 320 \pmod{p}$.)

55) Let $a(x) = x^3 + x + 1$ and $b(x) = x^2 + x$. Determine $\gcd(a(x), b(x))$ and find polynomials u, v such that $u(x)a(x) + v(x)b(x) = \gcd(a(x), b(x))$. (This is the same old Euclidean algorithm but with polynomial division.)

56) For each $1 \le a < 24$ with $\gcd(a, 24) = 1$ determine $\mathrm{OrderMod}_{24}(a)$. Is there a primitive element (i.e. an element of order $\varphi(24) = 8$)? Compare the frequency of orders occurring with the case of a prime modulus (where there are $\varphi(k)$ elements of order k).

57) We are working over the ring $\mathbb{Z}_3$ of integers modulo 3. Consider the matrices

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 2 & 1 & 2 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \\ 2 & 1 & 2 & 1 \end{pmatrix}$$

You are given the information that A has order 80 and that B is a power of A. Using the discrete logarithm methods (Pohlig Hellman, Hensel-Lifting) seen in class, find e such that $A^e = B$. (In GAP you can enter these matrices as

```
A:=[[0,0,0,1],[1,0,0,0],[0,1,0,0],[0,0,1,2]]*One(GF(3));
B:=[[0,2,1,2],[0,0,2,1],[0,0,0,2],[2,1,2,1]]*One(GF(3));
```

and instead of a Babystep/Giantstep algorithm you may solve the small remaining discrete logarithm problems $C^x = D$ as

```
x:=First([1..16],x->C^x=D);
```

58) a) Let p be an odd prime and $p-1 = 2^k \cdot q$ with q odd and let $1 \le a < p$ such that $a^q \not\equiv 1 \pmod{p}$. Show that $\mathrm{OrderMod}_p(a^q)$ must be even.
b) Show that for such an a you have that one of a^q, a^{2q},..., $a^{2^{k-1}q}$ will be congruent to -1 modulo p. (**Hint:** Problem 47)
c) Let m be an odd number with $m-1 = 2^k \cdot q$ with q odd and $a < m$ such that $a^q \not\equiv 1 \pmod{m}$. Show that if $a^{2^l q} \not\equiv -1 \pmod{m}$ for any $0 \le l < k$ then m cannot be a prime. (This is called the *Miller-Rabin test* for compositeness. It can be shown that this test has a high chance of success — at least 75% of all values of a will work— if m is composite.)
d) Let $m = 294409 = 2^3 \cdot 36801$ and let $a = 2$. Then $2^{36801} \equiv 512 \not\equiv 1 \pmod{m}$. Calculate $512^2, 512^4$ mod m and conclude that m cannot be prime.

59) Did you feel any of the problems on the midterm were surprising or required too hard calculations? (This problem has no wrong answer. I am curious to know as I am teaching this class for the first time.)

Practice Problems: **2.11**, **2.12**, **2.29**, **2.30**, **2.34**, **3.4**, **3.13**, **3.14**,

Groups, Rings and Fields

Mathematicians have introduced names for certain structural arithmetic properties that arise in many places, trying to get a general framework to discuss the properties of such sets with arithmetic. They are modeled initially on sets of numbers you know, such as rational or complex numbers or integers. These structures are studied in detail in MATH 366, however it is useful to have some of the language available here.

In all cases we have a *set* A of objects and one or two operations (typically called + and $\cdot$) that take two elements of the set and produce a new one in the set A. (They are called *binary operations*, and we say that the set is *closed under these operations*.) What is important is that we *label* these operations as "addition" or "multiplication", but they might in fact not be the usual operations from arithmetic.

We also often look at two special kinds of elements, *neutral elements* and *inverses*; these are used to formulate the reverse operations, subtraction and division.

The following description aims to give the axiom sets in a context, they are not minimal[1].

Groups

A *Group* is a set $(A, \cdot)$ with one binary operation, usually called *multiplication* $a \cdot b$. We demand that

Associativity For any three elements $a, b, c \in A$ we have that $(ab)c = a(bc)$, that is we can dispense with parentheses when multiplying.

Identity There is one special element $e \in A$ (called the *One*, or the *Identity* element) such that $ae = a = ea$ for all $a \in A$.

Inverse For every element a there exists an element (usually denoted as a^{-1}) such that $aa^{-1} = e = a^{-1}a$.

[1] i.e. one could drop the requirement of some properties as they are implied by the others

These axioms are modeled on symmetry transformations, and indeed one primary use of groups is to describe symmetries with particular constraints.

Examples:

- The set of invertible matrices in a given dimension over a particular coefficient domain, e.g. $\mathrm{GL}_3(\mathbb{R})$.
- Invertible matrices with determinant one: $\mathrm{SL}_3(\mathbb{R})$.
- Orthogonal matrices. $O_3(\mathbb{R})$.
- Permutations on the numbers $\{1, \ldots, n\}$: S_n.

and of course all examples in the following section.
The definition of element *order*, that is the smallest $n > 0$ such that $a^n = 1$, is pertinent to any group, as is the formula for the order of a power a^k. If the group is finite every element order divides the group order. (In groups this is called Lagrange's theorem. We have seen special cases of this as Fermat's little theorem or Euler's theorem.)

Abelian Groups/Commutative Group

We take the axioms for a group, adding the condition (**Commutativity**), that is that $a \cdot b = b \cdot a$ for all $a, b \in A$. Because of this, sometimes people denote the binary operation by a +-symbol. Also the identity element then is often called a *Zero*.
A group in which all elements can be written as power of a particular element (a *primitive element*) is called *cyclic*. It automatically is abelian (as $a^e \cdot a^f = a^{e+f} = a^{f+e} = a^f \cdot a^e$). We have asserted that for a prime p, $U(Z_p)$ is cyclic. In this course we basically have only seen abelian groups. In particular the discrete logarithm problem lives natively in cyclic groups – one can consider other abelian groups for Diffie-Hellman-type key exchanges, and one can use the methods we have seen (Baby-Step/Giant-Step, Pohlig-Hellman, Hensel Lifting) for solving discrete logarithm problems in these other groups.

Examples:

- Integers under addition: $\mathbb{Z}$.
- Nonzero rationals under multiplication: $\mathbb{Q}^*$.
- Integers modulo m under addition: $(\mathbb{Z}_m, +)$.
- Integers $< m$ with $\gcd(a, m) = 1$ under multiplication modulo m: The *units* of $\mathbb{Z}_m$: $U(\mathbb{Z}_m) = U(m)$. (For prime m this is the setting of Diffie-Hellman. For nonprime m this is the setting of RSA.)
- A vector space is an (additive) group, together with multiplication by scalars (from a field, see below).

One reason for using the group $U(m)$ is that it provides good security, having elements of large order and thus a hard discrete logarithm problem. Also the operation in this group is suitable for tiny computers (e.g. chipcards which only get power from one sweep of radio waves), that is it is comparatively easy to implement and requires few processor cycles. There are other groups which have the same, or even better properties. One such example are groups associated to geometric structures called *Elliptic curves*. For these structures there exist cryptosystems that are the analogues of Diffie-Hellman or El-Gamal, just implemented on a different group.
The methods we have seen for solving discrete logarithm problems: Babystep/Giantstep, Pohlig-Hellman, and Hensel Lifting all only use the groupstructure and thus are applicable to any group.

Rings

Matrices, Integers, Rationals, Reals,
Polynomials and all their Ideals,
Real valued functions and similar things,
These are a few of my favorite rings.

With rings we introduce a second operation. A ring $(A, +, \cdot)$ is a set with two binary operations, such that

Additive Group The set A with the addition $+$ forms an additive group.

Distributive Laws Addition and multiplication interact to allow to expand parenthetical sums: $(a + b)c = ac + bc$ and $a(b + c) = ab + ac$.

Multiplicative Identity (Some people leave this out of their definition and distinguish *Rings* and *Rings-With-One*.)

If multiplication commutes $ab = ba$ we call the structure a *commutative ring*.
Caveat: In some rings, e.g. $\mathbb{Z}_m$ we can have zero divisors, e.g. $ab = 0$ with $a, b \neq 0$. If none exist, the ring is called an *Integral Domain*.

Examples:

- Integers $\mathbb{Z}$.
- Integers modulo m $(\mathbb{Z}_m, +, \cdot)$.
- $n \times n$ Matrices with entries over a ring.
- Polynomials with coefficients over a ring. $\mathbb{Q}[x]$, $\mathbb{Z}_m[x]$.
- Formal power series

The Euclidean algorithm lives in a subclass of integral domains (so-called *Euclidean rings*) and thus works for integers but also for polynomials. Similarly the concept of factorizations and irreducible elements (prime numbers) can be generalized to rings.
The setup of discrete logarithm and RSA only utilizes the group structure of $\mathbb{Z}_m^*$, but many factorization algorithms inherently use the additive structure (i.e. the ring properties) as well.

Fields

The axioms of a ring don't include division. We get this with the following structure: A set $(A, +, \cdot)$ is called a *field* if A is a commutative ring (with one) and the nonzero elements A^* form a commutative group with the 1 as identity.

Examples:

- $\mathbb{Q}, \mathbb{R}$
- $\mathbb{Z}_p$ for p prime.
- Field extensions: $\mathbb{C} = \mathbb{R}[i]$. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mod a, b \in \mathbb{Q}\}$.
- Other finite fields. (There is exactly one field of order p^n for each prime power p^n. For $n = 1$ these are $\mathbb{Z}_p$. For $n > 1$ they are formed similarly to $\mathbb{Q}[\sqrt{2}]$.

Linear algebra can be done over any field (not just $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ as seen in MATH369).