USS: Introduction to mathematical cryptography
Monday July 18 problems

Your focus today should be on setting yourself up for success this week, and how to do that will depend on your background. Therefore the problems below are grouped by topic, and you should work on the problems you think you would most benefit from.

Operations modulo p

If n is any integer, we write $a \equiv b \pmod{n}$ (read "a is equivalent to b modulo n") if and only if n divides $a - b$. The set of equivalence classes modulo n form a ring which we denote $\mathbb{Z}/n\mathbb{Z}$.

1. Basic operations modulo p: Let $p = 31$, and perform the following computations. For each operation, give your answer as a **least residue**, i.e., give the representative of your answer which is between 0 and 30, inclusively.

   (a) $19 + 17 \pmod{31}$

   (b) $16 \times 5 \pmod{31}$

   (c) $2^5 \pmod{31}$

2. Prove that if p is a prime and p divides the product ab, then p must either divide a or it must divide b.

3. Prove that if p is prime, then every nonzero element in $\mathbb{Z}/p\mathbb{Z}$ is a unit.

4. Inverses modulo p: When p is prime and $a \not\equiv 0 \pmod{p}$, we can compute the inverse of $a \pmod{p}$, denoted $a^{-1} \pmod{p}$, by following these three steps:

   A. Perform the Euclidean algorithm to compute the gcd of a and p.

   B. Since p is prime and $a \not\equiv 0 \pmod{p}$, the greatest common divisor is 1. Backsubstitute in the Euclidean algorithm to solve the equation $ax + py = 1$.

   C. We have that $ax \equiv 1 \pmod{p}$, so $a^{-1} \equiv x \pmod{p}$.

   By any method you choose, compute the following quantities. Please give your answer as a least residue.

   (a) $7^{-1} \pmod{13}$

   (b) $2^{-1} \pmod{41}$

   (c) $17^{-1} \pmod{101}$

   (d) $47^{-1} \pmod{97}$

5. Show that if $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$.

Theory of cyclic groups

A **group** $(G, \cdot)$ is a set G equipped with a binary operation $\cdot$, which we usually call "multiplication," such that the following are true:

- There exists an element $e \in G$ such that $e \cdot g = g \cdot e = g$ for each $g \in G$.
- For all $f, g, h \in G$, we have $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.
- For all $g \in G$, there is $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

We often only write G for a group $(G, \cdot)$ if the operation is understood.

A group G is **cyclic** if there is an element $g \in G$ such that every element of G can be written in the form g^n for some integer n. Here by "g^n" we mean $g \cdot g \cdot \dots \cdot g$, multiplied with itself n times if n is positive, or $g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}$, multiplied with itself $-n$ times if n is negative, and with the convention that $g^0 = e$. In that case we write $G = \langle g \rangle$ and say that G is **generated by** g.

It is a fact that, up to isomorphism, there is a unique cyclic group of order n for each positive integer n, which we denote C_n. There is also a unique cyclic group of infinite order, which is isomorphic to $(\mathbb{Z}, +)$.

1. Let $G = \langle g \rangle$. Prove that the element $g^n \in G$ has order $\frac{\#G}{\gcd(n,\#G)}$, where $\#G$ is the cardinality of the set underlying G.
2. Prove that if $G = \langle g \rangle$, then $G = \langle g^n \rangle$ if and only if $\gcd(n, \#G) = 1$.
3. Prove that a cyclic group G has $\varphi(\#G)$ distinct generators, where φ is the Euler-totient function.
4. Prove that every subgroup of a cyclic group is cyclic.
5. Prove that for every positive integer d dividing n, C_n contains exactly one subgroup isomorphic to C_d.

Field theory

An **abelian group** is a group G such that $g \cdot h = h \cdot g$ for all $g, h \in G$.

A **field** $(F, +, \cdot)$ is a set F such that

- $(F, +)$ is an abelian group, with identity denoted 0;
- for $F^\times$ the set of nonzero elements of F, $(F^\times, \cdot)$ is also an abelian group, with identity denoted 1; and
- for all $a, b, c \in F$, we have $a \cdot (b + c) = a \cdot b + a \cdot c$.

It is a fact that $F[x]$, the ring of polynomials in one variables over a field F, is a Euclidean domain; that is, for every pair of polynomials $f(x), g(x) \in F[x]$ with $g(x) \neq 0$, we can write

$$f(x) = q(x) \cdot g(x) + r(x), \quad \text{with } \deg r(x) < \deg g(x) \text{ or } r(x) = 0,$$

in a unique way. We call $q(x)$ the **quotient** of the division of $f(x)$ by $g(x)$ and we call $r(x)$ the **remainder** of the division of $f(x)$ by $g(x)$.

1. Show that if F is a field, $a \in F$ and $f(x) \in F[x]$, we have that $f(a) = 0$ if and only if the remainder of the division of $f(x)$ by $x - a$ is zero.

2. Show that if F is a field and $f(x) \in F[x]$, there are at most $\deg f$ distinct elements a of F such that $f(a) = 0$.

3. Now let $F = (\mathbb{Z}/p\mathbb{Z}, +, \times)$ for p a prime; this is a field. Use problem 3 of the Operations modulo p section to show that every element $a \in F^\times$ is a root of the polynomial $f(x) = x^{p-1} - 1$. Conclude that $f(x) = x^{p-1} - 1$ has exactly $p - 1$ distinct roots in F.

4. Prove that if $F = \mathbb{Z}/p\mathbb{Z}$, then $(F^\times, \times)$ is a cyclic group.