Set 6

(A) Euler's φ-function

(1) What are the values of $\varphi(2)$, $\varphi(3)$, $\varphi(4)$, $\varphi(5)$, $\varphi(6)$, $\varphi(7)$ and $\varphi(8)$?

(2) Show that, for an integer $n > 1$, $\varphi(n)$ is the number of integers a with $1 \leq a < n$ with $\gcd(a, n) = 1$. We write this as:

$$\varphi(n) = \#\{a \in \mathbb{Z} \mid 1 \leq a < n \text{ and } \gcd(a, n) = 1\}$$

(3) Compute $\varphi(n)$ for $n = 5, 25, 125, 7, 49, 35, 245, 175$. Any observations? If p is prime and $a \geq 1$ is an integer, what is $\varphi(p^a)$?

(4) Evaluate the sum $\sum_{d|n} \varphi(d)$ for $n = 1, 2, 3, \ldots, 8$. Any conjectures? Can you prove your conjecture when n is prime? How about when $n = p^2$? How about $n = p^a$ where $a \geq 1$ is an integer?

(5) For each unit u of $\mathbb{Z}/6$, what is $u^{\varphi(6)}$ in $\mathbb{Z}/6$? Do the same in $\mathbb{Z}/n$ for $n = 2, 3, 4, 5$. Any conjectures? How is this conjecture related to our previous conjectures about units and their orders in $\mathbb{Z}/n$?

(B) More group theory, and an application to groups of units

(1) Let G be a finite group, take an element $a \in G$ and consider the subset $H_a = \{e, a, a^2, a^3 \cdots\}$ (note that, since G is finite, so is H_a).

(2) (***HW***) Show that the size of H_a is equal to the order of a.

(3) Show that H_a is a subgroup of G; see Set 5 (F).

(4) Given another element $b \in G$, the *left coset* of b with respect to H_a is the subset $bH_a = \{b, ba, ba^2, \cdots\}$. Is bH_a always a subgroup?

(5) Show the following:

- (i) The left coset bH_a has as many elements as H_a; that is, $\#(bH_a) = \#H_a$.
- (ii) For yet another element $c \in G$, we have $c \in bH_a$ if and only if $cH_a = bH_a$.
- (iii) The group G is a disjoint union of left cosets. This means that we can find elements $b_1, \cdots, b_s \in G$ such that

$$G = b_1 H_a \cup \cdots \cup b_s H_a$$

and such that $b_i H_a$ and $b_j H_a$ share no elements whenever $i \neq j$.

- (iv) The number of elements of H_a divides the number of elements of G, and thus the order of a divides the number of elements of G.

(6) Let $n > 1$ be an integer. Show that for every $a \in (\mathbb{Z}/n)^\times$, the order of a divides $\varphi(n)$, as we conjectured last week. How does this relate to (A5)?

(7) Prove Fermat's little theorem: for every integer a and every prime p, we have $a^p \equiv a \mod p$; that is, $a^p - a$ is divisible by p.

(C) Polynomial rings, and division with remainder

(1) Expand the product $(x^2 + 3x + 2)(2x + 1)$ in $\mathbb{Z}/5[x]$?

(2) You may have encountered "polynomial long division" before. Apply it to the fraction

$$\frac{x^3 + 7x + 1}{2x^2 + x - 1}$$

in $\mathbb{Q}[x]$ to find $q(x)$ and $r(x)$ with $x^3 + 7x + 1 = q(x)(2x^2 + x - 1) + r(x)$.

(3) Repeat the previous step, but now working on $\mathbb{Z}/3[x]$.

(4) Can you do it in $\mathbb{Z}/4[x]$?

(5) What conditions on our number system ensure we can perform polynomial long division? For example, we have seen it works in $\mathbb{Q}[x]$, but not in $\mathbb{Z}/4[x]$. Explain why it always work in $\mathbb{Z}/p[x]$ when p is a prime number.

(6) (***HW***) Show that $(x^2+x+1)(x+2) = x^3+2$ in $\mathbb{Z}/3[x]$. Note that this is not true in $\mathbb{Q}[x]$! In which of the following number systems is the polynomial $f(x) = x^3+2$ irreducible (i.e. does not factor into a product of polynomials both of degree strictly less than 3)? Prove your claim. [Hint: if it did split, what would be the degrees of the factors? Use this to show the polynomial would have to have a root]

- (i) $\mathbb{Q}[x]$
- (ii) $\mathbb{Z}/5[x]$
- (iii) $\mathbb{Z}/7[x]$

(7) Convince yourself that if $p(x)$ is a polynomial of degree d over a field F then $p(x)$ can have at most d roots in F. [Hint: if you have a root α, consider long division by $x-\alpha$]

(D) Mathematical induction.

(1) Write down a proof of the statement

$$\text{for every } n \geq 1, \sum_{i=1}^{n} i = \frac{n(n+1)}{2},$$

by using mathematical induction.

(2) (***HW***) Find a similar formula for $\sum_{i=1}^{n} i^2$ for any integer $n \geq 1$, and prove it by using induction.

(3) Consider the ring $\mathbb{Z}[x,y]$ of polynomials in two variables x and y with integer coefficients.

- (i) Show that for any integer $n \geq 1$, there are integers C_k^n, for $0 \leq k \leq n$, such that

$$(x+y)^n = \sum_{k=0}^{n} C_k^n x^k y^{n-k}.$$

(e.g., $(x+y)^2 = x^2+2xy+y^2$, so $C_0^2 = 1$, $C_1^2 = 2$, $C_2^2 = 1$.) Show moreover that the integers C_k^n satisfy the relation

$$C_k^{n+1} = C_{k-1}^n + C_k^n.$$

- (ii) Next show that the integers C_k^n satisfy

$$C_k^n = \frac{n!}{k!(n-k)!},$$

where for any integer n, $n! = 1 \cdot 2 \cdots n$. (The C_k^n are referred to as binomial coefficients, and are usually written $\binom{n}{k}$.) Notice: we know that C_k^n is an integer, even though it is not clear at all from this formula!

- (iii) Convince yourself that (i) and (ii) are still true for any two elements x, y in an arbitrary commutative ring.
- (iv) Compute the binomial coefficients $\binom{p}{k}$ modulo p for various primes p and integers $0 \leq k \leq p$. What do you observe? Prove your observation.
- (v) Show by induction that for every integer a, $a^p \equiv a \pmod{p}$. [Hint: use (iv)]