Steven Rosendahl
Homework 8

1. Determine whether each of the following polynomials has a zero in the given $\mathbb{Z}_p$. Either find a zero or prove that no zero exists.

   (a) $f(x) = x^3 + x^2 + x + 1$ in $\mathbb{Z}_2$.

   We can factor $x^3 + x^2 + x + 1$ into $(x^2 + 1)(x + 1)$. The only two options for a root in $\mathbb{Z}_2$ are 1 and 0. If we plug in zero we get $(0 + 1)(0 + 1) \equiv 1 \mod 2$, so 1 is not a zero of the polynomial. If we try 1, we get $(1 + 1)(1 + 1) \equiv (2)(2) \equiv (0)(0) \equiv 0 \mod 2$, so 1 is a zero of the polynomial.

   (b) $f(x) = x^3 + x^2 + x + 1$ in $\mathbb{Z}_3$.

   $f(x)$ factors into $(x^2 + 1)(x + 1) \equiv (x^2 - 2)(x - 2) \mod 3$. We have one zero at $x = 2$. If we test 0, we get $(0 + 1)(0 + 1) \equiv 1 \mod 3$, so 0 is not a zero of the polynomial, and if we test 1 we get $(-1)(-1) \equiv 1 \mod 3$, so 1 is not a zero either.

   (c) $f(x) = x^2 + 2x + 3$ in $\mathbb{Z}_5$.

   The polynomial $f(x) = x^2 + 2x + 3$ cannot be factored in $\mathbb{Z}_5$. Therefore, it has no zeros since we cannot express it in the form $g(x)(x - \alpha)$.

2. Let $f(x) = x^2 + 1$. Prove that f has a zero in $\mathbb{Z}_5$, but not in $\mathbb{Z}_7$.

   If we consider the polynomial in $\mathbb{Z}_5$, we have that

   $$x^2 + 1 \equiv x^2 - 4 \equiv (x + 2)(x - 2) \equiv (x - 3)(x - 2) \mod 5.$$

   Since f was reducible in $\mathbb{Z}_5$, we know it has at least one zero, and in this case it has two zeros, $x = 3$ and $x = 5$. In $\mathbb{Z}_7$, we have

   $$x^2 + 1 \equiv x^2 - 6 \mod 7.$$

   The polynomial $x^2 - 6$ is irreducible in $\mathbb{Z}_7$, so there are no roots.

3. Suppose that p is prime, k is a non-zero element of $\mathbb{Z}_p$, and $f_k(x) = x^2 - k$.

   (a) Prove that s is a zero of f_k if and only if $-s$ is also a zero of f_k.

   $\Rightarrow$) Suppose s is a zero of f_k. Then $s^2 - k \equiv 0 \mod p$. If $-s$ is not a zero, then we have $(-s)^2 - k \not\equiv 0 \mod p$, so $s^2 - k \not\equiv 0 \mod p$, which is a contradiction.

   $\Leftarrow$) Suppose $-s$ is a zero of f_k. Then $(-s)^2 - k \equiv 0 \mod p$. Then $s^2 - k \equiv 0 \mod p$, and s is a zero of f_k, so $-s$ is a zero of f.

   (b) Further assuming that $p > 2$ prove that f_k either has no zeros in $\mathbb{Z}_p$ or exactly two zeros in $\mathbb{Z}_p$.

   Suppose there was only one zero in $\mathbb{Z}_p$. We know this cannot be the case, since by (a) we showed that if s is a zero, then $-s$ is also a zero. If we suppose there are more than 2 zeros, then we can consider another zero, σ. By (a), we know that $-\sigma$ is also a zero. Since $deg(f) = 2$, we know that there are at most 2 zeros in $\mathbb{Z}_p$. There cannot be just one zero, so there must be only two zeros, or no zeros.

4. Let p be a prime with $p > 2$ and assume that $a, b, c, r \in \mathbb{Z}_p$ with $a \not\equiv 0 \mod p$. Further, we define the polynomial $f(x) = ax^2 + bx + c \in \mathbb{Z}_p[x]$.

   (a) Prove that r is a zero of f in $\mathbb{Z}_p$ if and only if $(2ar + b)^2 \equiv b^2 - 4ac \mod p$.

   $\Rightarrow$) Since r is a zero of $f(x)$ and f is a quadratic polynomial, we can create the expression

   $$\begin{aligned} ar^2 + br + c &\equiv 0 \mod p \\ ar^2 + br &\equiv -c \mod p. \end{aligned}$$

Consider the term $(2ar+b)^2$. Then

$$\begin{aligned}(2ar+b)^2 &= 4a^2r^2 + 4bar + b^2 \\ &= 4a(ar^2+br) + b^2 \\ &= 4a(-c) + b^2 \\ &= b^2 - 4ac \\ &\equiv b^2 - 4ac \mod p\end{aligned}$$

$\Leftarrow$) Suppose $(2ar+b)^2 \equiv b^2 - 4ac \mod p$. Then

$$\begin{aligned}&4a^2r^2 + 4arb + b^2 \equiv b^2 - 4ac \mod p \\ &4a^2r^2 + 4arb \equiv -4ac \mod p \\ &4a^2r^2 + 4arb + 4ac \equiv 0 \mod p \\ &4a(ar^2 + br + c) \equiv 0 \mod p.\end{aligned}$$

Since we are in $\mathbb{Z}_p$, we know all elements have an inverse. We can multiply both sides of the congruence by $a^{-1}4^{-1}$, which gives us $ar^2 + br + c \equiv 0 \mod p$. Therefore, r is a root of f.

(b) A point $y \in \mathbb{Z}_p$ is called a *perfect square* if there exists $z \in \mathbb{Z}_p$ such that $z^2 = y$.

i. If f has at least one zero in $\mathbb{Z}_p$, prove that $b^2 - 4ac$ is a perfect square.

Suppose r is a zero of f. Then by (a) we have

$$(2ar+b)^2 \equiv b^2 - 4ac \mod p,$$

which implies $b^2 - 4ac$ is a perfect square.

ii. If $b^2 - 4ac \equiv 0 \mod p$, prove that f has a uniqe zero in f. Find a formula for that zero in terms of a and b.

Suppose $b^2 - 4ac \equiv 0 \mod p$. We know by (a) that r is root, and therefore $(2ar+b)^2 \equiv b^2 - 4ac \mod p$. Suppose ρ is a root of f. then $(2a\rho + b)^2 \equiv b^2 - 4ac \mod p$, so $(2ar+b)^2 \equiv (2a\rho+b)^2$. Since $b^2 - 4ac$ is a perfect square, then $2ar + b \equiv 2a\rho + b$. Then $2ar \equiv 2a\rho$, and multiplying by $2^{-1}a^{-1}$ yields $r \equiv \rho$. To find an expression for r, we know that $(2ar+b)^2 = 0$, so if we multiply by $(2ar+b)^{-1}$, we have $2ar + b = 0$. Then $r = -b2^{-1}a^{-1}$.

iii. If $b^2 - 4ac \not\equiv 0 \mod p$ and $b^2 - 4ac$ is a perfect square, prove that f has exactly two distinct zeros in $\mathbb{Z}_p$.

We know that we have the equivalence $(2ar+b)^2 \equiv b^2 - 4ac$. Let $x = (2ar+b)^2$ and $k = b^2 - 4ac$. Then we can rearrange the congruence to say $x^2 - k \equiv 0 \mod p$. We know $x^2 - k$ has either 0 or 2 zeros. Since k is a perfect square, we can let $k = j^2$ for some $j \in \mathbb{Z}_p$. Then $x^2 - k = x^2 - j^2 = (x+j)(x-j)$, which has two distinct roots in $\mathbb{Z}_p$.

5. Suppose that $g(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ and let ϕ be a zero of g.

(a) Prove that $\phi \notin \mathbb{Z}_3$.

Suppose that there is a zero of the polynomial $r \in \mathbb{Z}_3$. If $r = 0$, then we have $g = 1 \not\equiv 0 \mod 3$, so 0 is not a zero of the polynomial. If $r = 1$, then we have $g = 2 \not\equiv 0 \mod 3$. If $r = 2$, we have $2 \equiv -1 \mod 3$, so $g = (-1)^2 + 1 \equiv 2 \not\equiv 0 \mod 3$, so there are no zeros in $\mathbb{Z}_3$.

(b) Define the set $\mathbb{F}_9 = \{0, 1, 2, \phi, \phi+1, \phi+2, 2\phi, 2\phi+1, 2\phi+2\}$. Assuming that the multiplication and addition in $\mathbb{F}_9$ obeys the distributive law, prove that every non-zero element of $\mathbb{F}_9$ has a multiplicative inverse.

We know that ϕ is a zero of g, so we have that $\phi^2 + 1 = 0$, and $\phi^2 = 2$. Subtracting 1 from both sides yields $\phi^2 - 1 = 1$, so $(\phi + 1)(\phi - 1) = 1$. Therefore the inverse of $(\phi + 1)$ is $(\phi - 1)$. If we consider $\phi(2\phi)$, we get $2\phi^2 = 4 = 1$, so ϕ and 2ϕ are inverses. If we consider $(2\phi + 1)(2\phi + 2)$, we get $4\phi^2 + 4\phi + 2\phi + 2 = (1)(2) + \phi - \phi - 1 = 2 - 1 = 1$, so $(2\phi + 1)$ and $(2\phi + 2)$ are inverses. We also know that $(1)(1) = 1$, so 1 is its own inverse. Finally, $(2)(2) = 4 = 1$, so 2 is its own inverse as well.

6. If $p > 2$ is prime, prove that $\mathbb{Z}_p$ contains exactly $(p + 1)/2$ perfect squares.

Consider the set $S = \{\{x, -x\} | x \in \mathbb{Z}_p \text{ and } x \not\equiv 0 \mod p\}$. We first want to show that $x \not\equiv -x \mod p$.

Suppose $x \equiv -x \mod p$. Then $x \equiv (p - 1)x \equiv px - x \mod p$, so $2x \equiv xp \mod p$. We can multiply by x^{-1}, which yields $2 \equiv p \mod p$, so $p \equiv 2 \mod p$, which is a contradiction since $p > 2$. Therefore $x \not\equiv -x \mod p$.

We now need to show that every set $A \in S$ is disjoint with another set $B \in S$.

Suppose $A = \{x, -x\}$ and $B = \{y, -y\}$ with $A \cap B \neq \emptyset$. Take $z \in A \cap B$. Then $z \in A$ and $z \in B$. Suppose without loss of generality that $z \equiv x \mod p$ and $z \equiv y \mod p$. Then $x \equiv y \mod p$, so they are the same element.

We can now take every subset of S and square the elements within that set. Doing so gives for any subset $\{x^2, x^2\}$ which contains two equivalent perfect squares. We know that for every p there are $(p-1)/2$ of these sets, and that there is a trivial set $\{0, 0\}$, so there are $((p-1)/2)+1$, or $(p + 1)/2$ sets of perfect squares.