Units modulo a prime

1. For the following primes $p$, list all primitive roots of $(\mathbb{Z}/p\mathbb{Z})^\ast$. You may refer to the tables in Rosen’s text to produce one primitive root, but the rest should be computed by hand. Show your work.

   (a) $p = 19$
   (b) $p = 31$
   (c) $p = 43$

2. Fact: $5$ is a primitive root for $(\mathbb{Z}/97\mathbb{Z})^\ast$. List all elements of $(\mathbb{Z}/97\mathbb{Z})^\ast$ of order 16. You may express these as powers of 5, but you must justify your answer.

3. Let $p$ be an odd prime and suppose $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\ast$ is a primitive root. Prove that $\alpha^{p-1} = -1$.

4. For each of the following $f(x) \in \mathbb{Z}/13\mathbb{Z}$ find the number of roots $\alpha \in \mathbb{Z}/13\mathbb{Z}$ of $f(x)$. Justify your answer. It is possible to do each of these with little to no computation!

   (a) $f(x) = x^5 - 1$
   (b) $f(x) = x^4 + x^3 + x^2 + x + 1$. Hint: use the result above.
   (c) $f(x) = x^2 + 3x + 2$
   (d) $f(x) = x^6 + 12$

5. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial.

   (a) Prove that if $f(x)$ has an integer root, then $f(x)$ modulo $p$ has a root in $\mathbb{Z}/p\mathbb{Z}$ for all primes $p$.
   (b) Using the contrapositive of the implication in (a), show that $f(x) = x^3 - 8x^2 + 10x - 1$ has no integer roots.

6. Prove directly that if $n = p^r$ is a prime power, then $n = \sum_{d|n} \varphi(d)$.

7. Let $p$ be prime, and let $d \mid p - 1$, $d \neq 2$. Prove that

$$\prod_{\substack{\alpha \in (\mathbb{Z}/p\mathbb{Z})^\ast \atop \text{ord}(\alpha) = d}} \alpha = 1;$$

i.e., the product of all elements of order $d$ is 1. Hint: $\text{ord}(\alpha) = \text{ord}(\alpha^{-1})$.

8. Let $p$ be an odd prime.

   (a) Prove that $(\mathbb{Z}/p\mathbb{Z})^\ast$ has an element of order $d$ if and only if $p \equiv 1 \pmod{d}$. 


We say an element $\beta \in \mathbb{Z}/p\mathbb{Z}$ is a square if there is an $\alpha \in \mathbb{Z}/p\mathbb{Z}$ such that $\alpha^2 = \beta$. Prove that the following are equivalent:

i. $p \equiv 1 \pmod{4}$;
ii. $\mathbb{Z}/p\mathbb{Z}$ contains an element of order 4;
iii. $-1$ is a square in $\mathbb{Z}/p\mathbb{Z}$.

(Check that this is indeed true for various primes.)

Let $p$ be prime and suppose $\alpha$ is a primitive root of $(\mathbb{Z}/p\mathbb{Z})^*$. 

(a) Prove that the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ that are squares are precisely the elements $\beta = \alpha^i$ where $i$ is even.

(b) Prove that exactly half of the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ are squares.

Let $p$ be prime and suppose $\alpha$ is a primitive root of $(\mathbb{Z}/p\mathbb{Z})^*$.

We say an element $\gamma \in \mathbb{Z}/p\mathbb{Z}$ is an $r$-th power if there is a $\beta \in \mathbb{Z}/p\mathbb{Z}$ such that $\beta^r = \gamma$; in this situation we call $\beta$ an $r$-th root of $\gamma$.

In this problem we will see precisely which elements of $(\mathbb{Z}/p\mathbb{Z})^*$ admit $r$-th roots; more precisely for each element of $(\mathbb{Z}/p\mathbb{Z})^*$ we will see how to compute the number of $r$-th roots it has.

(a) Given $\gamma \in (\mathbb{Z}/p\mathbb{Z})^*$, we can write $\gamma = \alpha^i$ for some $i \in \mathbb{Z}$. Prove that $\gamma$ is an $r$-th root if and only if $(r,p-1) | j$. Prove further that if this is the case, then $\gamma$ has precisely $(r,p-1)$ distinct $r$-th roots. Hint: a possible $r$-root $\beta$ can also be written as $\beta = \alpha^i$ for some $i$.

(b) Prove that if $(r,p-1) = 1$, then every element of $(\mathbb{Z}/p\mathbb{Z})^*$ has a unique $r$-th root.

(c) List all 36-th powers of $(\mathbb{Z}/97\mathbb{Z})^*$. 

2