1. Recall that Wilson’s theorem states, for $p$ a prime, that $(p - 1)! \equiv -1 \mod p$. Prove Wilson’s theorem using primitive roots.

*Solution.* Suppose $g$ is a primitive root mod $p$. Every integer between 1 and $p - 1$ is congruent to a unique power $g^d$ for some $d, 0 < d \leq p - 1$. Thus, for odd $p$,

$$(p - 1)! = (p - 1)(p - 2) \cdots 3 \cdot 2 \cdot 1 \equiv \prod_{d=1}^{p-1} g^d \mod p$$

$\equiv g^{\sum_{d=1}^{p-1} d} \mod p$

$\equiv g^{\frac{p(p-1)}{2}} \mod p$

$\equiv \left(g^{\frac{p-1}{2}}\right)^p \mod p$

$g$ has order $p - 1$, so $g^{p-1}$ has order 2 and is thus $-1 \mod p$, so for odd $p$, $(p - 1)! \equiv (-1)^p \mod p \equiv -1 \mod p$. For $p = 2$ Wilson’s theorem is obvious.

2. (a) Show that $x = 10$ is a solution to $x^8 \equiv 1 \mod 73$ and $x = 2$ is a solution to $x^9 \equiv 1 \mod 73$. (*Hint:* $10^5 \equiv -10 \mod 73$)

*Solution.* Dividing the hint by 10, $10^4 \equiv -1 \mod 73$, so $10^8 \equiv 1 \mod 73$. Also, $2^9 \equiv 64 \cdot 8 \mod 73 \equiv -9 \cdot 8 \mod 73 \equiv 1 \mod 73$. 

(b) What are the orders of $x = 10$ and $x = 2 \mod 73$?

*Solution.* Since $10^8 \equiv 1 \mod 73$, the order must divide 8, so is 2, 4 or 8. But $10^4 \equiv -1 \mod 73$, so the order must be 8.

Similarly, the order of 2 is 3 or 9, but $2^3 \equiv 8 \mod 73$, so 2 has order 9.

(c) Prove that 20 is a primitive root mod 73.

*Solution.* The order of 20 divides 72 = $2^3 \cdot 3^2$, so if it isn’t primitive then the order must divide 36 or 24. However, $20^{36} \equiv 2^{36} \cdot 10^{36} \equiv 10^1 \not\equiv 1 \mod 73$ and $20^{24} \equiv 2^{24} \cdot 3^{24} \equiv 2^6 \not\equiv 1 \mod 73$. Thus, 20 is primitive.

Alternatively, 8 and 9 are coprime, so the order of $2 \cdot 10$ must be $8 \cdot 9 = 72$.

3. Suppose $p$ is an odd prime with $p \equiv 1 \mod 3$.

(a) Show using quadratic reciprocity that $\left(\frac{-3}{p}\right) = 1$.

*Solution.* We know that $\left(\frac{a}{p}\right) = 1$ if and only if $p \equiv \pm 1 \mod 12$. Since $p \equiv 1 \mod 3$, either $p \equiv 1 \mod 12$ or $p \equiv 7 \mod 12$. In the first case, $p \equiv 1 \mod 4$, so

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = (1) \cdot \left(\frac{p}{3}\right) = 1$$
In the second case, \( p \equiv 3 \mod 4 \), so

\[
\left( \frac{-3}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{3}{p} \right) = (-1) \cdot \left( \frac{p}{3} \right) = 1
\]

(b) Show that an element \( c \) of order 3 mod \( p \) exists.

\textit{Solution.} There’s a primitive root mod \( p \), so we know that for any \( d \mid p - 1 \) there are \( \phi(d) \) elements of order 3. In particular, since \( 3 \mid p - 1 \), there is an element \( c \) of order 3. Indeed, if \( g \) is a primitive root mod \( p \), \( g^{\frac{p-1}{3}} \) will have order 3.

(c) Show that if \( c \) has order 3, then \( (2c + 1)^2 \equiv -3 \mod p \).

\textit{Solution.} Since \( c^3 \equiv 1 \mod p \),

\[
c^3 - 1 \equiv (c - 1)(c^2 + c + 1) \equiv 0 \mod p
\]

and since \( c \not\equiv 1 \mod p \), \( c^2 + c + 1 \equiv 0 \mod p \), so

\[
(2c + 1)^2 \equiv 4c^2 + 4c + 1 \equiv 4(c^2 + c + 1) - 3 \equiv -3 \mod p
\]

4. Suppose \( q(x, y) = ax^2 + bxy + cy^2 \) is a quadratic form of discriminant \( d(q) = b^2 - 4ac \).

(a) Show that \( q(x, y) \) factors as \( q(x, y) = (\alpha_1 x + \beta_1 y)(\alpha_2 x + \beta_2 y) \) if and only if \( d(q) \) is a perfect square (possibly zero).

\textit{Solution.} (\( \Rightarrow \)) By a simple computation,

\[
q(x, y) = \alpha_1 \alpha_2 x^2 + (\alpha_1 \beta_2 + \alpha_2 \beta_1)xy + \beta_1 \beta_2 y^2
\]

\[
d(q) = (\alpha_1 \beta_2 + \alpha_2 \beta_1)^2 - 4\alpha_1 \alpha_2 \beta_1 \beta_2 = (\alpha_1 \beta_2 - \alpha_2 \beta_1)^2
\]

(\( \Leftarrow \)) If \( b^2 - 4ac = m^2 \), then \( a|b^2 - m^2 \) so we can write \( a = a_1 a_2 \) with \( a_1|b - m \) and \( a_2|b + m \). Then

\[
q(x, y) = \left( a_2 x + \frac{b + m}{2a_1} y \right) \left( a_1 x + \frac{b - m}{2a_2} y \right)
\]

(b) Show that \( q(x, y) \) factors as \( q(x, y) = d(\alpha x + \beta y)^2 \) if and only if its discriminant is 0.
Solution. \(\Rightarrow\) Again by a simple computation,
\[
q(x, y) = d(\alpha x^2 + 2\alpha\beta xy + \beta^2)
\]
\[
d(q) = d^2((2\alpha\beta)^2 - 4\alpha^2\beta^2)
\]
\(\Leftarrow\) Set \(d = \gcd(a, b, c)\), and write \(q(x, y) = d(a'x^2 + b'xy + c'y^2)\). If \(b'^2 - 4a'c' = 0\), then \(a', c'\) are coprime, so they must both be squares, \(a' = \alpha^2, c' = \beta^2\). Then
\[
q(x, y) = d(\alpha^2x^2 + b'xy + \beta^2y^2) = d(\alpha x + \beta y)^2
\]

(c) Suppose \(d(q) = 0\). Show that \(q\) represents all integers of the form \(dn^2\), where \(d = \gcd(a, b, c)\).

Solution. Since \(d(q) = 0\), again if we write \(q(x, y) = d(a'x^2 + b'xy + c'y^2)\) then \(a', c'\) are coprime, so writing \(q(x, y) = d(\alpha x + \beta y)^2\) as above \(\alpha, \beta\) are coprime. Thus for any \(n \in \mathbb{Z}\) there are integers \(x, y\) with \(n = \alpha x + \beta y\), and \(q\) represents \(dn^2\).

5. (a) Find the four properly reduced forms of discriminant \(-44\).

Solution. The four properly reduced forms of discriminant \(-44\) are \(q_1(x, y) = x^2 + 11y^2, q_2(x, y) = 2x^2 + 2xy + 6y^2, q_3(x, y) = 3x^2 + 2xy + 4y^2, q_4(x, y) = 3x^2 - 2xy + 4y^2\).

(b) For the following values of \(n\), find all proper representations (possibly none) of \(n\) by the forms in part (a).

(i) \(n = 5\).

Solution. Any prime that is represented is represented 4 times, and they are
\[
5 = q_3(-1, 1) = q_3(1, -1) = q_4(1, 1) = q_4(-1, -1)
\]

(ii) \(n = 13\).

Solution. There are no representations, since \(z^2 \equiv -44 \mod 4 \cdot 13\) has no solutions since \(-44\) is not a square mod 13:
\[
\left(\frac{-44}{13}\right) = \left(\frac{4}{13}\right) \left(\frac{-11}{13}\right) = \left(\frac{2}{13}\right) = -1
\]

(iii) \(n = 53\).

Solution. The four representations are
\[
53 = q_1(3, 2) = q_1(3, -2) = q_1(-3, 2) = q_1(-3, -2)
\]