MME 529 HW6

1. In Z_{11} some numbers have square roots. Which numbers do and what are the square roots?

$1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 5$, $5^2 = 3$, $6^2 = 3$, $7^2 = 5$, $8^2 = 9$, $9^2 = 4$, $10^2 = 1$.

The square roots of 1 are 1, 10.
The square roots of 3 are 5, 6.
The square roots of 4 are 2, 9.
The square roots of 5 are 4, 7.
The square roots of 9 are 3, 8.
The square root of 0 is 0.

2. In Z_p show that $x^2 \equiv (p-x)^2 \bmod p$. How does this help with square roots? Give 2 examples.

$x^2 \equiv (p-x)^2 \bmod p$ iff

$p \mid [x^2 - (p-x)^2]$ iff $p \mid [p(2x-p)]$.

Since this holds, $x^2 \equiv (p-x)^2 \bmod p$.

Once you find a square root, x, of x^2, you get the other: $p-x$.

$3^2 \equiv (7-3)^2 \bmod 7 \rightarrow \sqrt{2} = 3, 4$
$8^2 \equiv (13-8)^2 \bmod 13 \rightarrow \sqrt{12} = 8, 5$

3. Solve $17x \equiv 5 \bmod 29$.

First find $17^{-1} = y$ by solving $17y \equiv 1 \bmod 29$.
This holds for $29k = 17y - 1$ or
$17y + 29k = 1$.

$29 = 17 \cdot 1 + 12$
$17 = 12 \cdot 1 + 5$
$12 = 5 \cdot 2 + 2$
$5 = 2 \cdot 2 + 1$
$2 = 1 \cdot 2$

$5 - 2 \cdot 2 = 1$
$5 - (12 - 5 \cdot 2) \cdot 2 = 1$
$12(-2) + 5(5) = 1$
$12(-2) + (17 - 12)5 = 1$
$17(5) + 12(-7) = 1$
$17(5) + (29 - 17)(-7) = 1$
$17(12) + 29(-7) = 1$

$\therefore y = 17^{-1} = 12$

$12 \cdot 17 \cdot x \equiv 12 \cdot 5 \bmod 29$
$1 \cdot x \equiv 60 \bmod 29$
$x \equiv 2 \bmod 29$

This means $x = 2 + 29m$, $m \in \mathbb{Z}$
solves $17x \equiv 5 \bmod 29$.

Ex) $17 \cdot 2 = 34 \equiv 5 \bmod 29$
$17 \cdot 31 = 527 \equiv 5 \bmod 29$
$17 \cdot (-27) = -459 \equiv 5 \bmod 29$

4. If $ax \equiv ay \bmod n$, can we always cancel the a?

No - only if a^{-1} exists for the given n. This is the case iff $\gcd(a,n)=1$ so that we can solve the equation

$$ar + ns = 1 \quad \text{for some } r, s \in \mathbb{Z}.$$

For example, $\gcd(3,12) = 3 \neq 1$ and

$$3 \cdot 2 \equiv 3 \cdot 6 \bmod 12$$
$$2 \not\equiv 6 \bmod 12 .$$

However, $\gcd(5,12) = 1$ and

$$5 \cdot 2 \equiv 5 \cdot 14 \bmod 12$$
$$2 \equiv 14 \bmod 12 .$$

Note that if n is prime, a^{-1} exists for all $a \not\equiv 0 \bmod n$. This is one reason why working in $\mathbb{Z}_p$ makes life easier.

5. Simplify $889345234 \bmod 25$ without using long division.

Since $889345234 = 8893452{\cdot}00 + 34$,
$889345234 \equiv 34 \bmod 25 = 9$.

6. Predict using algebra which numbers have an inverse in $\mathbb{Z}_{15}$.

a has an inverse $b = a^{-1}$ iff
$ab \equiv 1 \bmod 15$ iff $15 \mid (ab-1)$ iff

$a \cdot b + 15k = 1$ has an integer solution
iff $\gcd(a, 15) = 1$. This means
$1, 2, 4, 7, 8, 11, 13,$ and 14 have inverses.

7. Solve $x^2 - 2x + 2 \equiv 0 \bmod 13$.

$x^2 - 2x + 2 = 13k$
$x^2 - 2x + (2 - 13k) = 0$

$x = (2 \pm \sqrt{4 - 4(2 - 13k)}) / 2$
$= (2 \pm \sqrt{52k - 4}) / 2$
$= (2 \pm 10)/2$ for $k = 2$ ← general solution
$= 6, -4 \rightarrow x = 6 + 13k, -4 + 13j, k, j \in \mathbb{Z}$

For $x \in \{0, \ldots, 12\}$
$x = 6, 9$ satisfy
$x^2 - 2x + 2 \equiv 0 \bmod 13$.

$(6+13k)^2 - 2(6+13k) + 2 = 26 + 13(2 \cdot 6 \cdot k + 13k^2 - 2 \cdot k) \equiv 0$.

$(-4+13j)^2 - 2(-4+13j) + 2 = 26 + 13(2 \cdot (-4) j + 13j^2 - 2 \cdot j) \equiv 0$.

8. Show that $a = 2$ is a generator of $\mathbb{Z}_{13}$. What about $a = 5$?

In $\mathbb{Z}_{13}$,

$2^1 = 2$ $\quad$ $2^5 = 6$ $\quad$ $2^9 = 5$

$2^2 = 4$ $\quad$ $2^6 = 12$ $\quad$ $2^{10} = 10$

$2^3 = 8$ $\quad$ $2^7 = 11$ $\quad$ $2^{11} = 7$

$2^4 = 3$ $\quad$ $2^8 = 9$ $\quad$ $2^{12} = 1$

This shows that each of $1, 2, \ldots, 12$ can be written as a power of 2, modulo 13.

$5^1 = 5$ $\quad$ $5^4 = 1$ $\quad$ $5^7 = 5^3 \cdot 5^4 = 8$

$5^2 = 12$ $\quad$ $5^5 = 5 \cdot 5^4 = 5$ $\quad$ $5^8 = 5^4 \cdot 5^4 = 1$

$5^3 = 8$ $\quad$ $5^6 = 5^2 \cdot 5^4 = 12$ $\quad$ $\vdots$

5 does not generate $\mathbb{Z}_{13}$.

$6^1 = 6$ $\quad$ $6^5 = 2$ $\quad$ $6^9 = 5$

$6^2 = 10$ $\quad$ $6^6 = 12$ $\quad$ $6^{10} = 4$

$6^3 = 8$ $\quad$ $6^7 = 7$ $\quad$ $6^{11} = 11$

$6^4 = 9$ $\quad$ $6^8 = 3$ $\quad$ $6^{12} = 1$

6 generates $\mathbb{Z}_{13}$. Also 9 generates $\mathbb{Z}_{13}$.

9. If ABCDEFGHI is a bank routing number,

$7A + 3B + 9C + 7D + 3E + 9F + 7G + 3H + 9I$
must be congruent to 0 modulo 10.

a) Show that 211872946 passes this criterion.

$7\cdot 2 + 3\cdot 1 + 9\cdot 1 + 7\cdot 8 + 3\cdot 7 + 9\cdot 2 + 7\cdot 9$
$+ 3\cdot 4 + 9\cdot 6 = 250 \equiv 0 \mod 10.$

b) Show that 011000138 passes this criterion.

$7\cdot 0 + 3\cdot 1 + 9\cdot 1 + 7\cdot 0 + 3\cdot 0 + 9\cdot 0 + 7\cdot 1$
$+ 3\cdot 3 + 9\cdot 8 = 100 \equiv 0 \mod 10$

c) My checking account also passes.

10. What does a^{-2} mean in $\mathbb{Z}_n$?

For $a \in \mathbb{Z}_n$, a^{-2} is the element in $\mathbb{Z}_n$ such that $a^2 \cdot a^{-2} \equiv 1 \bmod n$, where $a^2 \in \mathbb{Z}_n$ as well.