Basic Algebra 1
Solutions to Assignment 3

Problem 1 The simplest way to do this is to check all the cases, but to do less work we make the following observation: $ax \equiv b \mod (n)$ and $ay \equiv b \mod (n) \Leftrightarrow a(x-y) \equiv 0 \mod (b)$ (check it!). So if x is a solution of $ax \equiv b \mod (n)$ then the other solutions of the equation are of the form $x + a'$ where $n \mid aa'$. We have,
(a) $3 * 4 \equiv 12 \equiv 5 \mod (7)$ and there are no other solutions because 7 is prime.
(b) $3 * 4 \equiv 12 \equiv 1 \mod (11)$ and $x = 4$ is the only solution.
(c) $3 * 2 \equiv 6 \mod (15)$ so we have $x = 2$ is a solution but notice that $15 \mid 3 * 5$ and $15 \mid 3 * 10$ so we have that $x = 2 + 5 = 7$ is a solution and $x = 12$ is also a solution (moreover they are the only ones)
(d) We try for $x = 0, 1, 2, 3, 4, 5, 6$ and notice that none of these work, we can stop, why? We have that $6 * 7 \equiv 6 * 14 \equiv 0 \mod (21)$ so it follows that if y is a solution to our equation, we can chose $y < 21$ and we also have that $y - 7, y - 14$ is a solution, thus if there is a solution $21 > y > 6$ then there exists a solution $0 \leq y' \leq 6$ but we checked that there were none.

Remark In general one has the following result.

(i) The equation $ax \equiv b \mod m$ *is soluble iff* $gcd(a, m) \mid b$.
(ii) If this is so, then there are exactly $d = gcd(a, m)$ *solutions.*
(iii) Given x_0 *is one solution, then*

$$x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d}, \cdots, x_0 + (d-1)\frac{m}{d}$$

are the other solutions.

Problem 2 We compute the squares in $\mathbb{Z}_8$

$$\begin{aligned}
&0^2 = 0\\
&1^2 = 1\\
&2^2 = 4\\
&3^2 = 9 = 1\\
&4^2 = 16 = 0\\
&5^2 = 25 = 1\\
&6^2 = 36 = 4\\
&7^2 = 49 = 1
\end{aligned}$$

We see that the possible sums of three squares are:

$$0 + 0 + 0 = 0; 0 + 0 + 1 = 1; 0 + 1 + 1 = 2;$$

$$1 + 1 + 1 = 3; 0 + 0 + 4 = 4; 0 + 1 + 4 = 5; 1 + 1 + 4 = 6.$$

So seven can not be expressed as a sum of three squares in $\mathbb{Z}_8$.

Now suppose towards a contradiction that every integer could be expressed as a sum of three squares. Let $n \in [7]_8 \subset \mathbb{Z}$ where $[7]_8$ is the equivalence class of integers congruent to 7 mod(8). Then by our supposition $n = a^2 + b^2 + c^2$ for some $a, b, c \in \mathbb{Z}$, hence we have the congruence equation $a^2 + b^2 + c^2 \equiv n \equiv 7 \mod (8)$. This is a contradiction, it follows that some integers (in particular 7) can not be expressed as a sum of three squares. Note that 7 is the smallest integer that can not be expressed as the sum of three squares!

Problem 3 Show that $a^5 \equiv a \mod (30)$ for all integers a. We have the following equivalencies

$$\begin{aligned} & a^5 \equiv a \mod (30) \\ \Leftrightarrow\ & a^5 - a \equiv 0 \mod (30) \\ \Leftrightarrow\ & 30 \mid a^5 - a \end{aligned}$$

We also have that $30 \mid (a^5 - a)$ if and only if $2, 3$ and 5 divide $a^5 - a$. One side of this implication is clear i.e. if $30 \mid x$ then $2, 3$ and 5 also divide x. On the other hand suppose that $2, 3$ and 5 divide x. Then by the fundamental theorem of arithmetic we have the unique prime factorization $x = \pm 1 * 2^{\epsilon_1} * 3^{\epsilon_2} * 5^{\epsilon_3} * \ldots$ and in particular we find that $\epsilon_1, \epsilon_2, \epsilon_3$ are all at least 1. So $30 = 2 * 3 * 5$ divides x as well. (It is sometimes useful to think that a divides b if and only if b "contains" a's prime factorization.)

So if we show that $n \mid a^5 - a$ for all a when $n = 2, 3, 5$, we're done. So we check for each of them. I'll only do the case for $n = 5$, we need to check for $a = 0, 1, 2, 3, 4$. When $a = 0, 1$ the equation clearly holds. For the rest:

$$\begin{aligned} 4^5 = 4^2 * 4^2 * 4 &\equiv 1 * 1 * 4 \equiv 4 \mod (5) \\ 3^5 = 3^2 * 3^2 * 3 &\equiv (-1) * (-1) * 3 \equiv 3 \mod (5) \\ 2^5 = 4 * 2^3 &\equiv (-1) * 3 \equiv 2 \mod (5) \end{aligned}$$

So we have that for each $a \in \mathbb{Z}$, $a^5 \equiv a \mod (5)$. Similarly the equations also hold for all a modulo 2 and 3. We can therefore infer that for all $a \in \mathbb{Z}, a^5 \equiv a \mod (30)$.

Problem 4 We first consider $\mathbb{Z}_{11}$. We start checki and find that in $\mathbb{Z}_{11}$:

$$\begin{aligned} & 2 = 2 \\ & 2^2 = 4 \\ & 2^3 = 8 \\ & 2^4 = 16 = 5 \\ & 2^5 = 2 * 5 = 10 \\ & 2^6 = 2 * 10 = 9 \\ & 2^7 = 2 * 9 = 7 \\ & 2^8 = 2 * 7 = 3 \\ & 2^9 = 2 * 3 = 6 \\ & 2^{10} = 2 * 6 = 1 \end{aligned}$$

So 2 is a primitive root mod 11. And for the record, there is not really a nice way to find such roots.

For $\mathbb{Z}_{24}$ a totally different approach is in order, checking every elements will do the trick but it is too much work, especially because $\mathbb{Z}_{24}$ has no such primitive roots. The two next propositions illustrate what's going on.

Proposition 1: Let R be a commutative ring and suppose that $a, b \in R$ are such that $a, b \neq 0$ but $ab = 0$, then a may not have a multiplicative inverse.
Proof: Suppose that $a \neq 0$ did have a multiplicative inverse a^{-1} but that there was some $b \neq 0$ such that $ab = 0$.

$$\begin{aligned} b &= 1 * b \\ &= (a^{-1}a)b \\ &= a^{-1}(ab) = a^{-1} * 0 = 0 \\ &\quad \Rightarrow b = 0 \end{aligned}$$

Which is a contradiction.$\square$

Proposition 2: If every non-zero element of $\mathbb{Z}_n$ is a power of some $a \in \mathbb{Z}_n$, then all non-zero elements of $\mathbb{Z}_n$ have multiplicative inverses.
Proof: Let $x \in \mathbb{Z}_n$ be any nonzero element. Then for some $l, m \in \mathbb{N}$, $x = a^l$ and $a^m = 1$. We may assume that $l < m$ if not then for some k, $l \leq km$ and we have $a^{km} = (a^m)^k = 1^k = 1$ so we may replace m by km. Let $j = m - l \geq 0$ then we have that $xa^j = a^{l+j} = 1$, hence x has a multiplicative inverse. Since x is arbitrary the Proposition is proved. $\square$

Now we have in $\mathbb{Z}_{24}$ that $2 * 12 = 0$ so by Proposition 1, 2 or 12 may not have a multiplicative inverses. It then follows from Proposition 2 that $\mathbb{Z}_n$ has no primitive root.

Problems 5 and 6 If $x^2 \equiv 1$ in $\mathbb{Z}_n$ this means in particular that $n \mid (x^2 - 1)$ (look at Problem 3 if this isn't clear) which implies $n \mid (x + 1)(x - 1)$.

For Problem 5 suppose we can take $\mathbb{Z}_{80}$. Notice that $9^2 = 81 = 1$ but that $9 \neq 1, -1$. So we have a counterexample. By the way I picked 80 because $80 = (9 + 1)(9 - 1)$.

If $n > 2$ is prime, notice the following: Suppose there was some $[x] \in \mathbb{Z}_n$ such that $[x]^2 = [1]$. If $[x] \neq [1]$ or $[-1]$ then $[x + 1], [x - 1] \neq [0]$. Picking a representative $x_0 \in \mathbb{Z}$ from $[x]$ such that $x_0 < n$ gives us that in $\mathbb{Z}$, $n \mid (x_0 - 1)(x_0 + 1)$, and since n is prime it must divide one of the factors on the right, but notice that $x_0 - 1$ and $x_0 + 1$ are both nonzero and less than n, so n can't divide them which is a contradiction. We infer that the only possibilities for $[x]$ are $[1]$ and $[-1]$.

Problem 7 Suppose that $\gcd(a, n) = 1$ then there exist $p, q \in \mathbb{Z}$ such that $pa + qn = 1$. It follows that $pa + qn \equiv 1 \mod (n)$ so we can write

$$[pa] + [qn] = [1] \qquad (\star)$$

in Z_n. But note that the term $[qn] = [q][n] = [0][n] = [0]$. So in fact $(\star)$ yields $[p][a] = [1]$ therefore $[a]$ has the multiplicative inverse $[p]$.

On the other hand, suppose that $[a] \in \mathbb{Z}_n$ had a multiplicative inverse $[a']$, then picking a representative $a'_0 \in \mathbb{Z}$ of the equivalence class $[a']$ we get the congruence relation $aa_0' \equiv 1 \mod (n)$. So applying the division algorithm in $\mathbb{Z}$ we get $aa_0' = pn + 1$ for some $p \in \mathbb{Z}$ which implies $aa_0' - pn = 1$. We know that $\gcd(a, n)$ is the smallest strictly positive integer representable as a linear combination of a and n, so it follows that $\gcd(a, n) = 1$.

Problem 8 By Problem 7, the invertible elements in $\mathbb{Z}_5$ correspond to equivalence classes of elements relatively prime to 5, so they are $[1], [2], [3], [4]$. Similarly for $\mathbb{Z}_{12}$ the invertible elements are $[1], [5], [7], [11]$ i.e. everything relatively prime to 12.

Problem 9 First suppose that p is prime, and let $1 \leq k \leq p-1$. Since the binomial coefficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is an integer, therefore $k!(p-k)! \mid p \times (p-1)!$. Now since $p \nmid k!(p-k)!$ (convince yourself of this!), we infer that $\gcd(k!(p-k)!, p) = 1$. Thus $k!(p-k)! \mid (p-1)!$, and hence the binomial coefficient

$$\binom{p}{k} = p \times \frac{(p-1)!}{k!(p-k)!}$$

is a multiple of p, and we are done. [Note that we have used the fact that if $a \mid bc$ and if $\gcd(a, b) = 1$ then $a \mid c$.]

Now conversely, we suppose that all the binomial coefficients

$$\binom{n}{k}, \qquad (1 \leq k \leq n-1)$$

are multiples of n, and then prove that n must be prime. If not, let $p < n$ be a prime divisor of n. It follows from what we have assumed that

$$\frac{1}{n}\binom{n}{p} = \frac{(n-1)!}{p!(n-p)!} = \frac{(n-1)(n-2)\cdots(n-p+1)}{p!}$$

is an integer. This in turn implies that for some $1 \leq j \leq p-1$, $p \mid n-j$. On the other hand $p \mid n$, hence $p \mid j$ which is a contradiction!

Problem 10 Let $f(x) = x^p - x$. It is clear that $p \mid f(0)$ and that $p \mid f(1)$. Now we prove by induction that $p \mid f(n)$ for all n. For this let us look at $f(n+1)$:

$$f(n+1) = (n+1)^p - (n+1) = f(n) + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \cdots + \binom{p}{p-1}n.$$

It follows from previous problem and from our induction hypothesis that the right-hand side is divisible by p, so is the left-hand side and we are done!

Problem 11 First note that since $1729 = 7 \times 13 \times 19$, it is enough to prove separately

$$a^{1729} \equiv a \mod (7), \quad a^{1729} \equiv a \mod (13), \quad a^{1729} \equiv a \mod (19).$$

The idea is to repeatedly use Fermat's little theorem. We only do it for the first congruence relation as a sample and leave the other two for you. It is a good practice!

$$a^{1729} = (a^{247})^7 \equiv a^{247} = a^2(a^{35})^7 \equiv a^2a^{35} = a^2(a^5)^7 \equiv a^2a^5 \equiv a \mod (7).$$