21-128 and 15-151 problem sheet 7

Solutions to the following seven exercises and optional bonus problem are to be submitted through gradescope.

Problem 1

For $x, y, z \in \mathbb{Z}$, suppose that 5 divides $x^2 + y^2 + z^2$. Prove that 5 divides at least one of x, y or z.

Solution. Note that $0^2 = 0 \equiv 0 \bmod 5$, $(\pm 1)^2 \equiv 1 \bmod 5$ and $(\pm 2)^2 \equiv 4 \equiv -1 \bmod 5$. Hence all squares of integers are congruent to either 0, 1 or -1 modulo 5; moreover, given $a \in \mathbb{Z}$, $a^2 \equiv 0 \bmod 5$ if and only if $5 \mid a$.

Hence if 5 doesn't divide any of x, y or z, then each of x^2, y^2 or z^2 must be congruent to 1 or -1 modulo 5. But:

- $1 + 1 + 1 = 3 \equiv 3 \bmod 5$.
- $1 + 1 - 1 \equiv 1 \bmod 5$.
- $1 - 1 - 1 \equiv 4 \bmod 5$.
- $-1 - 1 - 1 \equiv 2 \bmod 5$.

So $x^2 + y^2 + z^2$ must be congruent to 1, 2, 3 or 4 modulo 5. Hence $5 \nmid x^2 + y^2 + z^2$. By contraposition, the claim in the question holds.

Problem 2

The base 10 representation of an integer is *palindromic* if the digits read the same when written forward or backward. Prove that every palindromic integer with an even number of digits is divisible by 11.

Solution. First note that given $n \in \mathbb{N}$, with n odd and $0 \leq i \leq n$, we have

$$10^{n-i} + 10^i \equiv (-1)^{n-i} + (-1)^i \bmod 11$$

Now $(-1)^{n-i} = (-1)^n(-1)^{-i} = -(-1)^i$. Hence

$$10^{n-i} + 10^i \equiv -(-1)^i + (-1)^i \equiv 0 \bmod 11$$

Hence $11 \mid 10^{n-i} + 10^i$.

Now if an integer a is palindromic in base 10 with an even number of digits, then it takes the form

$$a = \sum_{i=0}^{d} a_i(10^{2d+1-i} + 10^i)$$

for some digits a_i for $0 \leq i \leq 9$. By what we just proved, 11 divides each term in the sum, and hence $11 \mid a$.

Problem 3

Show your work in the following computations.

(a) Determine the last two digits of 14^{2022}.

(b) Compute $\frac{53!}{27}$ mod 27.

(c) Find all integers x such that $x^2 + 3x \equiv 3^{31} \mod 29$.

Solution.

(a) Euler's Thorem looks tempting here, but 14 and 100 aren't coprime. We can compute 14^{2022} mod 25, and determine what it is mod 100 from there. We compute that $\varphi(25) = 20$, so $14^{20} \equiv 1$ mod 25 by Euler's Theorem. Then $14^{2022} \equiv_{25} (14^{20})^{101} \cdot 14^2 \equiv_{25} 14^2 \equiv_{25} 196 \equiv_{25} -4$. We know that $4 \mid 4(2^{2020} \cdot 7^{2022}) = 14^{2022}$, so the ending must also be divisible by 4 (for any number $x = 100y + z$, $x \equiv z$ mod 4). So we're left with 4 possible endings if we add 25 to this: 21, 46, 71, and 96. $4(24) = 96$, and the ending of a number is unique, so the last two digits of 14^{2022} are 96.

(b) $\frac{53!}{27} = \prod_{i=1}^{26} i \cdot \prod_{i=28}^{53} i$, and since 27 divides the first factor, we see that $\frac{53!}{27}$ is congruent to zero, modulo 27.

(c) We know $3^{31} = 3^{28+3} \equiv 3^3$ mod $29 \equiv 27$ mod 29 by Fermat's Little Theorem.
So $x^2 + 3x \equiv 27$ mod $29 \iff x^2 + 3x + 2 \equiv 0$ mod $29 \iff (x+1)(x+2) \equiv 0$ mod 29.
By definition, $29 \mid (x+1)(x+2)$ and since 29 prime, $29 \mid (x+1)$ or $29 \mid (x+2)$.
So $x \equiv 28$ mod 29 or $x \equiv 27$ mod 29.

Substituting back in, we see that $(-1)^2 + 3(-1) \equiv_{29} -2 \equiv_{29} 3^{31}$ and $(-2)^2 + 3(-2) \equiv_{29} -2 \equiv_{29} 3^{31}$.

Problem 4

Show that the equation $x^2 + 1 \equiv 0 \pmod{p}$ has a solution when p prime and $p \equiv 1 \pmod{4}$.

Hint: Wilson's Theorem.

Solution. We know that $(p-1)! \equiv -1 \pmod{p}$ by Wilson's Theorem. Let A be the product of the first $\frac{p-1}{2}$ numbers in this factorial and let B be the product of the remaining numbers. By definition of A and B, we have that $AB = (p-1)!$.

For a small example, when $p = 13$, this looks like $A = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 6!$ and $B = 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \equiv (-6) \cdot (-5) \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) = (-1)^6 \cdot 6! \pmod{13}$.

In general, $A = (\frac{p-1}{2})!$, and $B = (-1)^{\frac{p-1}{2}} (\frac{p-1}{2})!$, since each term in B is the same as A but with an additional minus sign. However, since $p \equiv 1 \pmod{4}$, we see that $\frac{p-1}{2}$ is even, so $(-1)^{\frac{p-1}{2}} = 1$. Therefore, $A = B$, so $-1 \equiv (p-1)! = AB = A^2$ so setting $x = A$ satisfies $x^2 + 1 \equiv 0 \pmod{p}$.

Problem 5

Let m and n be positive, relatively prime integers, and r and s be integers such that $mr \equiv 1 \bmod n$ and $ns \equiv 1 \bmod m$. For integers a, b, find an integer value of x in terms of a, b, m, n, r, s satisfying $x \equiv a \bmod n$ and $x \equiv b \bmod m$.

Solution. $x \equiv a \bmod n$ if and only if $x = a + nk$ for some integer k. Substituting this into the second congruence, we have $a + nk \equiv b \bmod m$ which is equivalent to $nk \equiv b - a \bmod m$. To solve this last congruence, we multiply both sides by s to obtain $nsk \equiv k \equiv s(b-a) \bmod m$, which means that $k = s(b-a) + mj$ for some integer j. Thus $x = a + nk = a + ns(b-a) + nmj$ for some integer j. In particular, we can take $j = 0$ and verify that $x = a + ns(b-a)$ solves both congruences.

Problem 6

Let $A \subseteq \mathbb{N}^+$ and $B \subseteq \mathbb{N}^+$ be nonempty sets of positive integers. Define

$$A + B \stackrel{\text{def}}{=} \{a + b : a \in A, b \in B\}.$$

Show that $A + B$ is finite if and only if both A and B are finite.

Solution. We proceed to show that the condition is necessary and sufficient.

- $(\Rightarrow)$ Suppose $A + B$ is finite. We show that A is finite; showing that B is finite is analogous.

Fix $b \in B$. Define $\varphi : A \to A + B$ via

$$\varphi(a) = a + b \quad \text{for all } a \in A.$$

φ is well-defined and we claim that φ is an injection. To prove this, let $a_1, a_2 \in A$ and suppose that $\varphi(a_1) = \varphi(a_2)$. Then

$$a_1 + b = a_2 + b \quad \Rightarrow \quad a_1 = a_2.$$

So, indeed, φ is an injection. We have thus found an injection from A into a finite set, and so by Theorem 7.1.13 part (a), A must be finite.

- ($\Leftarrow$) Suppose A and B are finite. If A or B is empty, then $A + B$ equals B or A, and hence it is finite. Thus, we may assume that neither A nor B is empty. By Lemma 7.1.23, A and B must both have greatest elements. Let m_A denote the greatest element in A, and define m_B similarly. We claim that
$$A + B \subseteq [m_A + m_B].$$
This implies that $A + B$ is a subset of a finite set and thus must be finite. To prove this, let $x \in A + B$ be arbitrary. By definition, there exist $a \in A$ and $b \in B$ such that $x = a + b$. Then $1 \leq a \leq m_A$ and $1 \leq b \leq m_B$, so
$$1 < 2 \leq a + b \leq m_A + m_B \quad \Rightarrow \quad a + b \in [m_A + m_B].$$
Since x was arbitrary, we deduce that $A + B \subseteq [m_A + m_B]$, as desired.

Problem 7

For arbitrary $f : \mathbb{N} \to \mathbb{N}$ and $g : \mathbb{N} \to \mathbb{N}$, show that if the image of g is finite, then the image of $f \circ g$ is finite with size less than or equal to size of the image of g.

Solution. To show that the image of $f \circ g$ is finite with size less than or equal to size of the image of g, we surject the image of g onto it. Define $h : g[\mathbb{N}] \to (f \circ g)[\mathbb{N}]$ via $h(x) = f(x)$.

Well-definedness of h:

- Totality: h is clearly defined for all $x \in g[\mathbb{N}]$.
- Existence: For an arbitrary $x \in g[\mathbb{N}]$, by definition $\exists x' \in \mathbb{N}, g(x') = x$. Then necessarily $h(x) = f(x) = f(g(x'))$ for some $x' \in \mathbb{N}$, so $h(x) \in (f \circ g)[\mathbb{N}]$
- Uniqueness: There is only one possible output for every input x, namely, $f(x)$, which is unique by well definedness of f.

Surjectivity of h:

Fix $a \in (f \circ g)[\mathbb{N}]$. Then it follows from the definition of image that $\exists x \in \mathbb{N}, (f \circ g)(x) = a \implies f(g(x)) = a$. Then define $z = g(x)$ and note $z \in g[\mathbb{N}]$ by the definition of image. We then see that $s(z) = a$ as required for s to be a surjection.

Therefore, the image of $f \circ g$ is finite with size less than or equal to size of the image of g.

Bonus Problem - 2 points

Find all positive integers a for which there exist non-negative integers $x_0, x_1, \dots x_{2020}$ satisfying the equation

$$a^{x_0} = a^{x_1} + a^{x_2} + \cdots + a^{x_{2020}}.$$

Solution. The base $a = 1$ can not work for any choice of x's, so we assume that $a > 1$ and consider the equation mod $a - 1$. This yields that 1 is congruent to 2020 modulo $a - 1$, ie $a - 1 \mid 2019$, ie there is a positive integer k such that $2019 = (a - 1) \cdot k$.

Thus, $a - 1 = 1$, $a - 1 = 3$, $a - 1 = 673$, or $a - 1 = 2019$. That is to say, $a = 2$, $a = 4$, $a = 674$, or $a = 2020$. All four of these values of a can be seen to work by taking $x_0 = k$, and among $x_1, \dots, x_{2020}$ taking a of them to be 0, and taking $a - 1$ of them to be 1, $a - 1$ of them to be 2, $\dots$, $a - 1$ of them to be $k - 1$.