**M E T U  Department of Mathematics**

| **Math 123, Fall 2023, Midterm 2, December 15, 2023, 17:40** | | |
|---|---|---|
| FULL NAME | ID NUMBER | SIGNATURE |
| | | |
| 6 QUESTIONS ON 4 PAGES | | DURATION: 90 MINUTES |

**Q1.(20 points)** Find all integer solutions of the following system of congruences.

$$3x \equiv 9 \pmod{39}$$
$$8x \equiv 1 \pmod{15}$$
$$x \equiv 1 \pmod{8}$$

Observe that

- Since $\gcd(3, 39) = 3$, by a theorem proven in class, we have that $3x \equiv 9 \pmod{39}$ iff $x \equiv 3 \pmod{13}$.
- Since the multiplicative inverse of 8 modulo 15 is 2, we have that $8x \equiv 1 \pmod{15}$ iff $x \equiv 2 \pmod{15}$.

Consequently, solving the given system of congruences is equivalent to solving the following system of congruences.

$$x \equiv 3 \pmod{13}$$
$$x \equiv 2 \pmod{15}$$
$$x \equiv 1 \pmod{8}$$

The integers 8, 13 and 15 *are pairwise relatively prime* and hence, by the Chinese Remainder Theorem, this system of congruences has a solution that is unique modulo $8 \cdot 13 \cdot 15 = 1560$. We can find this unique solution following the proof of the Chinese Remainder Theorem. In order to do this, we first need to solve the linear congruences $120x \equiv 1 \pmod{13}$ and $104x \equiv 1 \pmod{15}$ and $195x \equiv 1 \pmod{8}$.

For the first congruence, we have $120x \equiv 3x \equiv 1 \pmod{13}$ and hence $x_1 = 9$ is a solution. For the second congruence, we have $104x \equiv -x \equiv 1 (\mathrm{mod}\ 15)$ and hence $x_2 = -1$ is a solution. For the third congruence, we have $195x \equiv 3x \equiv 1 \pmod{8}$ and hence $x_3 = 3$ is a solution. Therefore, by the proof of the Chinese Remainder Theorem,

$$x = 3 \cdot 120 \cdot 9 + 2 \cdot 104 \cdot -1 + 1 \cdot 195 \cdot 3 = 3617$$

is a solution to this system of congruences. Moreover, any other solution to this system is congruent to 3617 modulo 1560. For example, $497 \equiv 3617 \pmod{1560}$ is a solution.

**Q2.(15 points)** If they exist, find all integer solutions of the linear congruence

$$102x \equiv 30 \pmod{141}$$

that are incongruent modulo 141.

Since $\gcd(102, 141) = 3 \mid 30$, by a theorem proven in class, we know that the linear congruence $102x \equiv 30 \pmod{141}$ has 3 mutually incongruent solutions modulo 141. Indeed, given a particular solution $x_0$, we know that these 3 mutually incongruent solutions are $x_0$, $x_0 + \frac{141}{3}$ and $x_0 + \frac{2 \cdot 141}{3}$. So we need to find a particular solution.

Recall that any solution of the linear Diophantine equation $102x + 141y = 30$ induces a solution of the linear congruence $102x \equiv 30 \pmod{141}$ and vice versa. We now solve $102x + 141y = 30$ using the Euclidean algorithm.

$$\begin{aligned}
141 &= 102 \cdot 1 + 39 \\
102 &= 39 \cdot 2 + 24 \\
39 &= 24 \cdot 1 + 15 \\
24 &= 15 \cdot 1 + 9 \\
15 &= 9 \cdot 1 + 6 \\
9 &= 6 \cdot 1 + 3 \\
6 &= 3 \cdot 2 + 0
\end{aligned}$$

Starting from the last equation and writing the remainders of previous equations in the reverse order, we get that $3 = 102 \cdot 18 + 141 \cdot (-13)$ and hence $30 = 102 \cdot 180 + 141 \cdot (-130)$. Consequently, by taking the modulus of both sides with respect to 141, we obtain that

$$102 \cdot 39 \equiv 102 \cdot 180 \equiv 30 \pmod{141}$$

Hence 39 is a particular solution of $102x \equiv 30 \pmod{141}$. Therefore, 39, 86 and 133 are the 3 solutions that are incongruent modulo 141.

**Q3.(15 points)** Let $p$ be an odd prime number. Show that

$$2 \cdot 4 \cdots (2p-2) \equiv -1 \pmod{p}$$

Since $p$ is an odd prime, $p \nmid 2$ and hence, by Fermat's little theorem, we have that $2^{p-1} \equiv 1 \pmod{p}$. Moreover, by Wilson's theorem, we have $(p-1)! \equiv -1 \pmod{p}$. Combining these two congruences together with an algebraic manipulation of the given congruence, we get that

$$2 \cdot 4 \cdots (2p-2) \equiv (2 \cdot 1) \cdot (2 \cdot 2) \cdots (2 \cdot (p-1)) \equiv 2^{p-1} \cdot (p-1)! \equiv 1 \cdot (-1) \equiv -1 \pmod{p}$$

| FULL NAME | ID NUMBER | SIGNATURE |
|---|---|---|
| | | |

**Q4.(20 points)** Let $n$ be a positive integer. Show that $\sigma(n)$ is odd if and only if $n$ is a perfect square or twice a perfect square.

In the case that $n = 1$, the statement trivially holds as $\sigma(1) = 1$ and 1 is a perfect square. Thus, in the rest of the proof, we may assume that $n > 1$. By the Fundamental Theorem of Arithmetic, we can write $n = \prod_{i=1}^{r} p_i^{k_i}$ where $p_i$'s are prime numbers and $k_i$'s are positive integers. Moreover, we have proven in class that $\sigma(n) = \prod_{i=1}^{r}(1 + p_i + p_i^2 + \cdots + p_i^{k_i})$. Observe that $\sigma(n)$ *is odd if and only if each factor in this product is odd.* We now show both directions of the given equivalence.

$(\Rightarrow)$ : Suppose that $\sigma(n)$ is odd. Then each factor $(1+p_i+p_i^2+\cdots+p_i^{k_i})$ is odd. Observe that if $p_i$ is odd, then, in order for $(1+p_i+p_i^2+\cdots+p_i^{k_i})$ to be odd, we have to have an odd number of terms in this sum. Hence, *if $p_i$ is odd, then $k_i$ is even.* We split into two cases.

- Case I ($n$ is even): Then 2 is a prime factor of $n$. Without loss of generality, suppose that $p_1 = 2$. We know that, $k_i$ is even for each $2 \leq i \leq r$, say, $k_i = 2\ell_i$. We have the following two subcases:
  - If $k_1$ is even, say $k_1 = 2\ell_1$, then we have $n = \prod_{i=1}^{r} p_i^{k_i} = \prod_{i=1}^{r} p_i^{2\ell_i} = \left(\prod_{i=1}^{r} p_i^{\ell_i}\right)^2$ and so $n$ is a perfect square.
  - If $k_1$ is odd, say, $k_1 = 2\ell_1 + 1$, then we have $n = \prod_{i=1}^{r} p_i^{k_i} = 2\prod_{i=1}^{r} p_i^{2\ell_i} = 2\left(\prod_{i=1}^{r} p_i^{\ell_i}\right)^2$ and so $n$ is twice a perfect square.
- Case II ($n$ is odd): Then all prime factors of $n$ are odd and hence each $k_i$ is even, say, $k_i = 2\ell_i$. Consequently, we have $n = \prod_{i=1}^{r} p_i^{k_i} = \prod_{i=1}^{r} p_i^{2\ell_i} = \left(\prod_{i=1}^{r} p_i^{\ell_i}\right)^2$ and hence $n$ is a perfect square.

$(\Leftarrow)$ : Suppose that $n$ is a perfect square or twice a perfect square. We now split into these two cases:

- Case I ($n$ is a perfect square): In this case, $n$ has a prime factorization of the form $\prod_{i=1}^{r} p_i^{2\ell_i}$. But then, each term of the form $(1+p_i+p_i^2+\cdots+p_i^{2\ell_i})$ is odd and hence $\sigma(n)$ is odd.
- Case II ($n$ is twice a perfect square): In this case, $n$ has a prime factorization of the form $2\prod_{i=1}^{r} p_i^{2\ell_i}$ where we may assume $p_1 = 2$. Since $(1+2+2^2+\cdots+2^{2\ell_1+1})$ is odd and $(1+p_i+p_i^2+\cdots+p_i^{2\ell_i})$ is odd for each $2 \leq i \leq 2$, $\sigma(n)$ is odd.

**Q5.(10 points)** Show that the Diophantine equation $x^2+1 = 43y$ has no integer solutions.

Assume towards a contradiction that $x^2 + 1 = 43y$ has integer solutions, say, $x_0, y_0 \in \mathbb{Z}$. Then $x_0^2 + 1 = 43y_0$ and hence $x_0^2 + 1 \equiv 0 \pmod{43}$. Consequently, the quadratic congruence $x^2 + 1 \equiv 0 \pmod{43}$ has a solution in integers. Observe that 43 is prime. We know that the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$ a solution in an odd prime modulus $p$ if and only if $p$ is of the form $4k + 1$. Thus 43 is of the form $4k + 1$, which is a contradiction.

**Q6.(7+7+6 points)** Consider the number-theoretic function $f$ defined on the set of positive integers given by

$$f(n) = \sum_{d|n} \tau(d)$$

a) Show that $f$ is a multiplicative function.

We know from a theorem proven in class that $G(n) = \sum_{d|n} g(d)$ is multiplicative whenever $g$ is multiplicative. By another theorem proven in class, we already have that $\tau$ is multiplicative. Hence $f$ must be multiplicative.

b) Let $p$ be prime and $k$ be a positive integer. Show that $f\left(p^k\right) = \dfrac{(k+1)(k+2)}{2}$.

The positive divisors of $p^k$ are precisely the integers of the form $p^i$ where $0 \leq i \leq k$. Moreover, we have shown in class that $\tau(p^i) = i+1$. Therefore

$$f(p^k) = \sum_{d|n} \tau(d) = \sum_{i=0}^{k} \tau(p^i) = \sum_{i=0}^{k} (i+1) = \sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

c) Let $n \geq 2$ be a positive integer with prime factorization $n = p_1^{k_1} \cdots p_r^{k_r}$. Find an explicit formula for $f(n)$ that does not use the sigma notation.

Observe that $p_i^{k_i}$'s are pairwise relatively prime integers. By Part (a), $f$ is multiplicative and hence

$$f(n) = f\left(\prod_{i=1}^{r} p_i^{k_i}\right) = \prod_{i=1}^{r} f\left(p_i^{k_i}\right)$$

But now, by Part (b), we see that

$$f(n) = \prod_{i=1}^{r} f\left(p_i^{k_i}\right) = \prod_{i=1}^{r} \frac{(k_i+1)(k_i+2)}{2} = \frac{(k_1+1)(k_1+2)\cdots(k_r+1)(k_r+2)}{2^r}$$