Math 240 – Assignment 3


1. \textit{(Irrational numbers).} Prove that $\sqrt[3]{7}$ is irrational.

2. \textit{(Euclid’s algorithm).} Use Euclid’s algorithm to find
   
   (a) $\gcd(583, 297)$
   
   (b) $\gcd(1208, 252)$
   
   (c) $\gcd(55, 34)$

3. \textit{(Congruences).} Evaluate each of the following (showing your work).
   
   (a) $17^{2012} \pmod{13}$
   
   (b) $12^{1729} \pmod{36}$

4. \textit{(Modular equations).} Solve each of the following for the variable $x$ (showing your work).
   
   (a) $5x + 16 \equiv 0 \pmod{29}$
   
   (b) $232x \equiv 12 \pmod{599}$

5. \textit{(Pigeonhole principle).}
   
   (a) Given a subset $X \subset \{1, \ldots, 10\}$, define $s(X) = \sum_{x \in X} x$. For example, $s(\{1, 5, 8\}) = 1 + 5 + 8 = 14$. Prove that if we choose any 28 subsets of $\{1, \ldots, 10\}$, each containing at least one and at most 3 elements, there are two of these subsets $A$ and $B$ such that $s(A) = s(B)$.
   
   (b) Prove that if $n + 1$ integers are selected from $\{1, \ldots, 2n\}$ then the selection includes integers $a$ and $b$ such that $a|b$.

\textbf{Point values for questions}

1. 3 points

2. 2 points for each part (total 6 points)

3. 2 points for each part (total 4 points)

4. 2 points for each part (total 4 points)

5. 3 points for part a, 4 points for part b.

Total possible number of points for the assignment: 24.
Solutions

1. (Irrational numbers.) Suppose $\sqrt{7}$ is rational, so we can write $\sqrt{7} = a/b$, where $a$ and $b$ are positive integers. Then $7 = a^3/b^3$ so $a^3 = 7b^3$. By the uniqueness of prime factorizations, we can uniquely write $a$ as a product $p_1, \ldots, p_k$ where $p_1, \ldots, p_k$ are all primes (not necessarily distinct). Let $m$ be the number of the primes from $p_1, \ldots, p_k$ that equal 7. In other words, $m$ is such that $7^m \mid a$ but $7^{m+1} \not\mid a$. The prime factorization of $a^3$ is $p_1 \cdot p_1 \cdot p_2 \cdot p_2 \cdot \ldots \cdot p_k \cdot p_k \cdot p_k$, and so $7^{3m} \mid a^3$ but $7^{3m+1} \not\mid a^3$.

Now do the same calculation with $b$. Let $n$ be such that $7^n \mid b$ but $7^{n+1} \not\mid b$. Then $7^{3n} \mid b^3$ but $7^{3n+1} \not\mid b^3$. Since $a^3 = 7 \cdot b^3$ it follows that $7^{3n+1} \mid a^3$ but $7^{3n+2} \not\mid a^3$. By the calculation from the preceding paragraph, it follows that $7^{3m} = 7^{3n+1}$, so $3m = 3n + 1$, which is impossible since $3m$ is divisible by 3 and $3n + 1$ is not. We have therefore arrived at a contradiction, and our only assumption was that $\sqrt{37}$ was rational; it must therefore be that $\sqrt{37}$ is irrational.

2. (Euclid’s algorithm.)

(a) We have

\[
\begin{align*}
583 &= 297 + 286 \\
297 &= 286 + 11 \\
286 &= 26 \cdot 11 + 0
\end{align*}
\]

So gcd(583, 297) = 11.

(b) We have $1208 = 4 \cdot 252 + 0$ so gcd(1208, 252) = 0.

(c) We have

\[
\begin{align*}
55 &= 34 + 21 \\
34 &= 21 + 13 \\
21 &= 13 + 8 \\
13 &= 8 + 5 \\
8 &= 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{align*}
\]

So gcd(55, 34) = 1.

3. (Congruences)
(a) First, $17 \equiv 4 \pmod{13}$ so $17^{2012} \equiv 4^{2012} \pmod{13}$. Next, 13 is prime so by Fermat’s little theorem $4^{12} \equiv 1 \pmod{13}$. It follows that $17^{2012} \pmod{13} = 4^{2012 \cdot 167 + 8} \pmod{13} = 4^{8} \pmod{13}$.

Finally, $4^{8} = 2^{12 + 4} \equiv 2^{4} \pmod{13} = 3$, so $17^{2012} \pmod{13} = 3$.

(b) For this we note that $12^{2} = 144 \equiv 0 \pmod{36}$, so $12^{1729} \pmod{36} = ((12^{2})^{864} \cdot 12) \pmod{36} = 0 \pmod{36}$.

4. (Modular equations)

(a) We’ll first solve $5y \equiv 1 \pmod{29}$. First, we have $5^{6} = 30 \equiv 1 \pmod{29}$, so $y \equiv 6$.

Multiplying by 16, we get that $5^{16} \equiv 16 \pmod{29}$, and $16^{6} \equiv 9 \pmod{29}$, so $5^{9} \equiv 16 \pmod{29}$. Finally, multiplying by -1 we get that $5^{9} \equiv 16 \pmod{29}$, and $9 \pmod{29} = 20$, so $x \equiv 20$.

(b) First notice that since $232 = 4 \cdot 58$ and $12 = 4 \cdot 3$, this is the same as solving $58x \equiv 3 \pmod{599}$. We then use Euclid’s algorithm:

$$599 = 10 \cdot 58 + 19$$

$$58 = 3 \cdot 19 + 1$$

Working backwards we then have

$$1 = 58 - 3 \cdot 19$$

$$= 58 - 3 \cdot (599 - 10 \cdot 58)$$

$$= 31 \cdot 58 - 3 \cdot 599,$$

and so $58 \cdot 31 \equiv 1 \pmod{599}$. Multiplying by 3 it follows that $58 \cdot 93 \equiv 3 \pmod{599}$, so $x \equiv 93$.

5. Pigeonhole principle

(a) First, for any non-empty subset $X$ of $\{1, \ldots, 10\}$, we have $s(X) \geq 1$, and if $|X| \leq 3$ then $s(X) \leq 10 + 9 + 8 = 27$. It follows that there are at most 27 distinct possibilities (pigeonholes) for the sums $s(X)$ when $1 \leq |X| \leq 3$, so by the pigeonhole principle, if we choose 28 sets of size at least one and at most three, among the 28 choices there must be two sets $A$ and $B$ with $|A| = |B|$.

(b) We choose $n + 1$ distinct integers (pigeons); call them $a_{1}, \ldots, a_{n+1}$. Next, for each odd number between 1 and $2n$ (so for the numbers 1, 3, 5, 7, 11, 13, ..., $2n - 1$) we make a pigeonhole. Put a number $a_{i}$ into the pigeonhole for the odd number $2k + 1$ if $2k + 1$ is the largest odd divisor of $a_{i}$. For example, put $a_{i}$ into pigeonhole number 5 if $a_{i}$ is a multiple of 5, but is not a multiple of 7, 9, 11, ..., $2n - 1$.

Since there are more pigeons than pigeonholes, some pigeonhole must get two pigeons. Suppose for example that 5 gets two pigeons. Then there are numbers $a$ and $b$ which are both multiples of 5 but not of 7, 9, 11, ..., $2n - 1$. We must then have $a = 2^{c} \cdot 5$ for some $c$, and $b = 2^{d} \cdot 5$ for some $d$. If $c < d$ then we have $b = a \cdot 2^{d-c}$ so $a \parallel b$; on the other hand if $d < c$ then $a = b \cdot 2^{c-d}$, so $b \parallel a$.

More generally, if the pigeonhole $k$ gets two pigeons $a$ and $b$, (where $k$ is some odd number less than $2n$) then $a = 2^{c} \cdot k$ and $b = 2^{d} \cdot k$ for some $c$ and $d$, and we again get that either $a \parallel b$ or $b \parallel a$, depending on whether $c < d$ or $d < c$.