Math 465 Number Theory I, Spring Term 2025, Solutions 5

1. Solve the simultaneous congruences

$$x \equiv 3 \pmod 6$$
$$x \equiv 5 \pmod{35}$$
$$x \equiv 7 \pmod{143}$$
$$x \equiv 11 \pmod{323}$$

The general solution is given by $x \equiv 3m_1n_1+5m_2n_2+7m_3n_3+11m_4n_4 \pmod m$ where $m = 6.35.143.323 = 9699690$, $m_1 = m/6 = 1616615 \equiv 5 \pmod 6$, $m_2 = m/35 = 277134 \equiv 4 \pmod{35}$, $m_3 = m/143 = 67830 \equiv 48 \pmod{143}$, $m_4 = m/323 = 30030 \equiv 314 \pmod{323}$, $m_1n_1 \equiv 1 \pmod 6$, $m_2n_2 \equiv 1 \pmod{35}$, $m_3n_3 \equiv 1 \pmod{143}$, $m_4n_4 \equiv 1 \pmod{323}$. Thus $n_1 = 5$, $n_2 = 9$, $n_3 = 3$, $n_4 = 287$ and $x \equiv 3.1616615.5 + 5.277134.9 + 7.67830.3 + 11.30030.287 = 132949395 \equiv 6853425 \pmod{9699690}$.

2. Prove that if p is an odd prime and $0 < k < p$, then (assuming $0! = 1$) $(p-k)!(k-1)! \equiv (-1)^k \pmod p$.

By Wilson's theorem $-1 \equiv (p-1)! = (p-k)!(p-k+1)(p-k+2)\dots(p-k+(k-1)) \pmod p$ and $(p-k+1)(p-k+2)\dots(p-k+(k-1)) \equiv (-k+1)(-k+2)\dots(-k+(k-1)) = (-1)^{k-1}(k-1)! \pmod p$.

3. (i) Let $m \in \mathbb{N}$. Prove that $(y-1)(y^{m-1}+y^{m-2}+\cdots+y+1) = y^m-1$. (ii) Let $n \in \mathbb{N}$. Prove that $(x^2+1)(x^2-1)(x^{4n-4}+x^{4n-8}+\cdots+x^4+1) = x^{4n}-1$. (iii) Let p be a prime number with $p \equiv 1 \pmod 4$. Prove that $x^2 \equiv -1 \pmod p$ has exactly two solutions.

(i) We have $(y-1)(y^{m-1}+y^{m-2}+\cdots+y+1) = y^m+y^{m-1}+\cdots+y-y^{m-1}-y^{m-2}-\cdots-y-1 = y^m-1$. (ii) We have $x^4-1 = (x^2+1)(x^2-1)$. Take $y = x^4$ and $m = n$ in (i). (iii) Let $n = \frac{p-1}{4}$. Then $x^{4n}-1 = x^{p-1}-1 \equiv 0 \pmod p$ whenever $x \not\equiv 0 \pmod p$, so $x^{4n}-1 \equiv 0 \pmod p$ has at least $p-1 = 4n$ solutions. By Lagrange's theorem $x^2+1 \equiv 0 \pmod p$, $x^2-1 \equiv 0 \pmod p$ and $x^{4n-4}+x^{4n-8}+\cdots+x^4+1 \equiv 0 \pmod p$ have at most 2, 2 and $4n-4$ solutions respectively. But then, by (ii), $x^2+1 \equiv 0 \pmod p$ must have at least $4n-(4n-4)-2 = 2$ solutions.

An alternative solution of (iii) not using (ii) goes as follows. Let g be a primitive root modulo p. Then $g^{(p-1)/2} \not\equiv 1 \pmod p$ and $(g^{(p-1)/2})^2 = g^{p-1} \equiv 1 \pmod p$, so $g^{(p-1)/2} \equiv -1 \pmod p$. Thus $(\pm g^{(p-1)/4})^2 \equiv g^{(p-1)/2} \equiv -1 \pmod p$.

4. Prove that if a has order 3 modulo a prime p, then $1+a+a^2 \equiv 0 \pmod p$, and $1+a$ has order 6.

We have $a^3 \equiv 1 \pmod p$, but $a^3-1 = (a-1)(a^2+a+1)$ and $a \not\equiv 1 \pmod p$. Thus $p|a^2+a+1$. We also have $(1+a)^2 = 1+2a+a^2 \equiv a \pmod p$. Hence $(1+a)^6 \equiv a^3 \equiv 1$, so $1+a$ has order dividing 6. But $a \not\equiv 0 \pmod p$, so from above $1+a$ does not have order 1 or 2. Finally $(1+a)^3 \equiv a(1+a) \equiv -1 \pmod p$, so $1+a$ does not have order 3.