Problem Set 5
Solutions

Foundations of Number Theory

Math 435, Fall 2006

1. (10+10 pts.)
   (a) Suppose n satisfies the given divisibility conditions. Then $3|n$ yields the existence of $k \in \mathbb{Z}$ with $n = 3k$. By $5|(n+2)$ we get $3k \equiv 3 \bmod 5$ and thus $k \equiv 1 \bmod 5$. Write $k = 5l+1$ with $l \in \mathbb{Z}$. Then $n = 15l+3$, and substituting into the third condition gives $l \equiv 0 \bmod 7$. Write $l = 7m$ with $m \in \mathbb{Z}$. Then $n = 3 + 105m$. So the smallest solution $n > 3$ is $n = 3 + 105 = 108$.
   (b) Proceeding similarly to (a) we get $n = 62$.
2. (20 pts.) Since $1 = (-1)\cdot 5+2\cdot 3$, hence $-5 \equiv 1 \bmod 3$, and $-2 \equiv 1 \bmod 3$, the first congruence is equivalent to $x \equiv 1 \bmod 3$. Similarly $1 = (-2)\cdot 4+9$ and hence $(-2)\cdot 4 \equiv 4 \bmod 3$, and $(-2)\cdot 7 \equiv 4 \bmod 9$, so the second congruence is equivalent to $x \equiv 4 \bmod 9$. Note that if $x \equiv 4 \bmod 9$ then $x \equiv 4 \bmod 3$ and thus $x \equiv 1 \bmod 3$. So the system consisting of the first two congruences has the solutions $x = 4 + 9k$ where $k \in \mathbb{Z}$. The last congruence is equivalent with $x \equiv 2 \bmod 5$. Substituting $x = 4+9k$ yields $9k \equiv 8 \bmod 5$. Now $1 = (-1)\cdot 9 + 2 \cdot 5$ and hence $k \equiv -8 \equiv 2 \bmod 5$. Write $k = 2+5l$ where $l \in \mathbb{Z}$, hence $x = 4+9(2+5l) = 22+45l$. Therefore the common solutions to the three congruences are $22 + 45l$ with $l \in \mathbb{Z}$.
3. (10 pts.) Let $d \in \mathbb{Z}$ with $d \equiv 3 \bmod 4$, and suppose for a contradiction that $(x, y) \in \mathbb{Z}^2$ satisfy $x^2 - dy^2 = -1$. The reducing mod 4 we have $-d \equiv -3 \equiv 1 \bmod 4$ and $-1 \equiv 3 \bmod 4$, hence $x^2+y^2 \equiv x^2-dy^2 \equiv -1 \equiv 3 \bmod 4$. By checking each pair $(x, y) \in \mathbb{Z}^2$ with $0 \le x \le y < 4$ one sees that the congruence $x^2 + y^2 \equiv 3 \bmod 4$ has no solution, in contradiction to our original assumption.
4. (10 pts.) By the Euler Criterion:
   $$\left(\frac{2}{11}\right) \equiv 2^{\frac{11-1}{2}} \equiv 2^5 \equiv 32 \equiv -1 \mod 11.$$
   Hence 2 is not a quadratic residue mod 11. Thus the congruence $x^2 \equiv 2 \bmod 77$ cannot have a solution.
5. (10 pts.) Let p be a prime with $p \equiv 1 \bmod 12$. By the Quadratic Reciprocity Law we have
   $$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}} \, (-1)^{\frac{3-1}{2}} = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}.$$

Now $p \equiv 1 \bmod 3$, hence p is a quadratic residue mod 3, so $\left(\frac{p}{3}\right) = 1$. Also $p \equiv 1 \bmod 4$, hence $\frac{p-1}{2}$ is even, so $(-1)^{\frac{p-1}{2}} = 1$. Therefore $\left(\frac{3}{p}\right) = 1$, i.e., 3 is a quadratic residue mod p.

6. (10 pts.) Let $a \in \mathbb{Z}$, and let $p > 3$ be a prime divisor of $a^2 + 3$. Then -3 is a quadratic residue mod p. Now

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right),$$

and by the Quadratic Reciprocity Law:

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}} = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}.$$

Since p is odd we have

$$(-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} = (-1)^{p-1} = 1$$

and hence

$$1 = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = (-1)^{p-1}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Thus p is a quadratic residue mod 3, hence $p \equiv 1 \bmod 3$.

7. (10 pts.) For $p = 3$: $7 \cdot 13 \cdot 19$. For $p = 5$: $5 \cdot 13 \cdot 17$. For $p = 7$: $7 \cdot 13 \cdot 19$.

8. (10 pts.) We have $385 = 5 \cdot 7 \cdot 11$. Quadratic residues mod 5: 0, 1, 4; quadratic residues mod 7: 0, 1, 2, 4; quadratic residues mod 11: 0, 1, 3, 4, 5, 9. So it is enough to choose a with $a \equiv 1 \bmod 5$, $a \equiv 2 \bmod 7$, $a \equiv 3 \bmod 11$, e.g., $a = 366$.

9. (20 pts. extra credit.) Let $p > 2$ be a prime. We have

$$\begin{aligned}
1!\,2!\,3!\cdots(p-1)! &= 1!\,3!\,5!\cdots(p-2)! \cdot 2!\,4!\,6!\cdots(p-1)! \\
&= \big(1!\,3!\,5!\cdots(p-2)!\big)^2 \cdot 2 \cdot 4 \cdot 6 \cdots (p-1) \\
&= \big(1!\,3!\,5!\cdots(p-2)!\big)^2 \cdot 2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!
\end{aligned}$$

and hence

$$1!\,2!\,3!\cdots(p-1)! \equiv \big(1!\,3!\,5!\cdots(p-2)!\big)^2 \cdot (-1)^{\frac{p^2-1}{8}} \cdot \left(\frac{p-1}{2}\right)! \bmod p \quad (1)$$

since

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \bmod p,$$

as shown in class. For $k = 1, \ldots, p-1$ we have

$$\begin{aligned}
(p-k)! &\equiv (p-k)(p-(k+1))\cdots(p-(p-1)) \\
&\equiv (-k)(-(k+1))\cdots(-(p-1)) \\
&\equiv (-1)^{p-k} \cdot k \cdot (k+1) \cdots (p-1) \\
&\equiv (-1)^{p-k} \cdot \frac{(p-1)!}{(k-1)!} \mod p
\end{aligned}$$

and hence

$$(p-k)! \cdot k! \equiv (-1)^{p+k}\,(p-1)!\,k \equiv (-1)^{p+k+1}\,k \mod p$$

where in the last congruence we used Wilson's Theorem. Grouping $(p-k)!$ and $k!$ for $k = 1, \ldots, (p-1)/2$ together, this yields

$$1!\,2!\,3! \cdots (p-1)! \equiv (-1)^e \left(\frac{p-1}{2}\right)! \mod p \tag{2}$$

where

$$e = \sum_{k=1}^{(p-1)/2} p + k + 1 = \frac{p(p-1)}{2} + \frac{(p-1)(p+1)}{8} + \frac{p-1}{2} = \frac{5(p^2-1)}{8}.$$

Note that

$$(-1)^e = \left((-1)^5\right)^{\frac{p^2-1}{8}} = (-1)^{\frac{p^2-1}{8}}.$$

Hence by (1) and (2):

$$\big(1!\,3!\,5! \cdots (p-2)!\big)^2 \equiv 1 \mod p.$$

The claim follows.

Total: 100 pts. + 20 pts. extra credit.