Number Theory

Homework 6

Kenny Roffo

Due March 7, 2016

1) If $\gcd(a, 30) = 1$, show that 60 divides $a^4 + 59$.

[I know there must be a better way to do this, but after many hours this was the best I could come up with]

Let a be an integer such that $(a, 30) = 1$. Then none of 2, 3 and 5 may divide a. Thus $a \equiv x \pmod{60}$ where $0 \leq x < 60$ and none of 2, 3 and 5 divide x. We see $a^4 \equiv x^4 \pmod{60}$, so we examine the value of $x^4 \pmod{60}$ for all possible values of x:

$$
\begin{aligned}
x = 7 : &\quad 7^4 \equiv 2401 \equiv 60(40) + 1 \equiv 1 \pmod{60} \\
x = 11 : &\quad 11^4 \equiv 14641 \equiv 1 \pmod{60} \\
x = 13 : &\quad 13^4 \equiv 1 \pmod{60} \\
x = 17 : &\quad 17^4 \equiv 1 \pmod{60} \\
x = 19 : &\quad 19^4 \equiv 1 \pmod{60} \\
x = 23 : &\quad 23^4 \equiv 1 \pmod{60} \\
x = 29 : &\quad 29^4 \equiv 1 \pmod{60} \\
x = 31 : &\quad 31^4 \equiv 1 \pmod{60} \\
x = 37 : &\quad 37^4 \equiv 1 \pmod{60} \\
x = 41 : &\quad 41^4 \equiv 1 \pmod{60} \\
x = 43 : &\quad 43^4 \equiv 1 \pmod{60} \\
x = 47 : &\quad 47^4 \equiv 1 \pmod{60} \\
x = 49 : &\quad 49^4 \equiv 1 \pmod{60} \\
x = 53 : &\quad 53^4 \equiv 1 \pmod{60} \\
x = 59 : &\quad 59^4 \equiv 1 \pmod{60}
\end{aligned}
$$

So no matter what, $a^4 \equiv 1 \pmod{60}$. But also $a^4 \equiv 1 \equiv -59 \pmod{60}$ which implies $60x | a^4 + 59$.

2) If $7 \nmid a$, prove that either $a^3 + 1$ or $a^3 - 1$ is divisible by 7.

Let a be an integer which is not divisible by 7. Then $a \equiv x \pmod 7$ where $x \in \{1, 2, 3, 4, 5, 6\}$. Now we examine the different cases for x:

$$\begin{aligned}
x = 1 : &\quad a^3 \equiv 1^3 \equiv 1 \pmod 7 \\
x = 2 : &\quad a^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod 7 \\
x = 3 : &\quad a^3 \equiv 3^3 \equiv 27 \equiv -1 \pmod 7 \\
x = 4 : &\quad a^3 \equiv 4^3 \equiv 64 \equiv 1 \pmod 7 \\
x = 5 : &\quad a^3 \equiv 5^3 \equiv 125 \equiv -1 \pmod 7 \\
x = 6 : &\quad a^3 \equiv 6^3 \equiv 216 \equiv -1 \pmod 7
\end{aligned}$$

No matter what x is, it is apparent that a^3 is congruent to either 1 or -1 (mod 7), which means by definition that 7 divides either $a^3 + 1$ or $a^3 - 1$.

3) The three most recent appearances of Halley's comet were in the years 1835, 1910, and 1986; the next occurrence will be in 2061. Prove that

$$1835^{1910} + 1986^{2061} \equiv 0 \pmod 7$$

We begin by noting that $1835 \equiv 1 \pmod 7$ and $1986 \equiv 5 \pmod 7$. This means

$$1835^{1910} + 1986^{2061} \equiv 1^{1910} + 5^{2061} \equiv 1 + 5^{2061} \pmod 7$$

Now we examine 5^{2061}. We know by Fermat's Little Theorem that $5^6 \equiv 1 \pmod 7$, and $(5^6)^n \equiv 1^n \equiv 1 \pmod 7$. Applying this, we see

$$5^{2061} = 5^{6(343)+3} = (5^6)^{343}5^3 \equiv (1)^{343}5^3 \equiv 125 \equiv 6 \pmod 7$$

And applying this result we have

$$1835^{1910} + 1986^{2061} \equiv 1 + 6 \equiv 7 \equiv 0 \pmod 7$$

And we are done.

4) If p and q are distinct primes, prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

Let p and q be distinct primes. By Fermat's Little Theorem we know $p^{q-1} \equiv 1 \pmod q$ and $q^{p-1} \equiv 1 \pmod p$ which means there exist integers x and y such that

$$qx = p^{q-1} - 1 \qquad\qquad py = q^{p-1} - 1$$

Multiplying and manipulating we see

$$\begin{aligned}
& qxpy = \left(p^{q-1} - 1\right)\left(q^{p-1} - 1\right) \\
\implies \quad & qxpy = p^{q-1}q^{p-1} - p^{q-1} - q^{p-1} + 1 \\
\implies \quad & p^{q-1}q^{p-1} - qxpy = p^{q-1} + q^{p-1} - 1 \\
\implies \quad & pq\left(p^{q-2}q^{p-2} - xy\right) = \left(p^{q-1} + q^{p-1}\right) - 1
\end{aligned}$$

This gives us the result we want as long as $p^{q-2}q^{p-2} - xy$ is an integer. Since q and p are prime, they are at least 2, thus the exponents are both at the very least 0, so it is true that $p^{q-2}q^{p-2} - xy$ is an integer. So pq divides $\left(p^{q-1} + q^{p-1}\right) - 1$, which means

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$