Assignment 6.

This homework is due *Thursday* March 1.

There are total 41 points in this assignment. 36 points is considered 100%. If you go over 36 points, you will get over 100% for this homework and it will count towards your course grade.

Collaboration is welcome. If you do collaborate, make sure to write/type your own paper *and give credit to your collaborators in your pledge.* Your solutions should contain full proofs. Bare answers will not earn you much.

(1) [2pt] (5.2.1) Use Fermat's theorem to verify that 17 divides $11^{104}+1$.

(2) (5.2.2ac)
   (a) [3pt] If $\gcd(a,35)=1$, show that $a^{12}\equiv 1 \pmod{35}$. (*Hint:* From Fermat's theorem $a^6\equiv 1 \pmod 7$ and $a^4\equiv 1 \pmod 5$.)
   (b) [3pt] If $\gcd(a,133)=\gcd(b,133)=1$, show that $133 \mid a^{18}-b^{18}$.

(3) [3pt] (5.2.3) From Fermat's theorem deduce that, for any integer $n\ge 0$,
$$13 \mid 11^{12n+6}+1.$$

(4) [2pt] (5.2.7+) If $p=2m+1$ is an odd prime and $p\nmid a$, prove that a^m-1 or a^m+1 is divisible by p. (*Hint:* Consider the product of these numbers.)

(5) [3pt] (5.2.18b) For $n=195=3\cdot 5\cdot 13$, prove that $a^{n-2}\equiv a \pmod n$ for any integer a.

(6) (5.2.10) Assuming a and b are integers not divisible by the prime p, establish the following:
   (a) [3pt] If $a^p\equiv b^p \pmod p$, then $a\equiv b \pmod p$.
   (b) [4pt] If $a^p\equiv b^p \pmod p$, then $a^p\equiv b^p \pmod{p^2}$.
   (*Hint:* By (a), $a=b+pk$ for some k, so that $a^p-b^p=(b+kp)^p-b^p$; now show that p^2 divides the later expression.)

(7) [4pt] (5.2.14) If p and q are distinct primes, prove that
$$p^{q-1}+q^{p-1}\equiv 1 \pmod{pq}.$$

(8) [3pt] (5.3.1a) Find the remainder when 15! is divided by 17.

(9) [3pt] (5.3.3) Arrange the integers $2,3,4,\dots,21$ in pairs a,b that satisfy $ab\equiv 1 \pmod{23}$.

(10) [4pt] (5.3.9) Using Wilson's theorem, prove that for any odd prime p,
$$1^2\cdot 3^2\cdot 5^2\cdots(p-2)^2\equiv(-1)^{(p+1)/2} \pmod p.$$
(*Hint:* Using that $k\equiv -(p-k) \pmod p$, show that
$$2\cdot 4\cdot 6\cdots(p-1)\equiv(-1)^{(p-1)/2}1\cdot 3\cdot 5\cdots(p-2) \pmod p.)$$

(11) [4pt] (5.3.18) Prove that if p and $p+2$ are a pair of twin primes, then
$$4((p-1)!+1)+p\equiv 0 \pmod{p(p+2)}.$$