MTH 305: Practice assignment 5

1 Fermat's little theorem

Establish the following assertions.

(i) $17 \mid 11^{104} + 1$.

(ii) For $n \geq 0$, $13 \mid 11^{12n+6} + 1$.

(iii) If $\gcd(a, 133) = \gcd(b, 133) = 1$, then $133 \mid a^{18} - b^{18}$.

(iv) $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$, for all a.

(v) $a^9 \equiv a \pmod{30}$, for all a.

(vi) If p is a prime and $\gcd(a, p) = 1$, then $x \equiv a^{p-2}b \pmod{p}$ is a solution to the congruence $ax \equiv b \pmod{p}$.

(vii) If a and b are integers not divisible by a prime p and $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.

(viii) If p is an odd prime, then

$$\sum_{i=1}^{p-1} i^p \equiv 0 \pmod{p}.$$

(ix) When $n = 2p$, where p is an odd prime, then $a^{n-1} \equiv a \pmod{n}$ for any integer a.

(x) If p and q are distinct primes, then

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

(xi) Any absolute pseudoprime is square-free.

(xii) Composite numbers of following forms are pseudoprime.

(a) $2^p - 1$, where p is prime.

(b) $2^{2^n} + 1$, for $n \geq 1$.

(xiii) Any integer of the form

$$(6k+1)(12k+1)(18k+1)$$

is an absolute pseudoprime when all three factors are prime.

2 Wilson's theorem

Establish the following assertions.

(i) When p is a prime,

$$(p-1)! \equiv p-1 \pmod{\sum_{i=1}^{p-1} i}.$$

(ii) When p is a prime, for any integer a, $p \mid (p-1)!a^p + a$.

(iii) For any odd prime p,

$$1^2 \cdot 3^2 \cdot 5^2 \ldots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

(iv) If $p = 4k+3$ is a prime and $a^2 + b^2 \equiv 0 \pmod{p}$, then $a \equiv b \equiv 0 \pmod{p}$.

(v) If $p = 4k+3$ is a prime, then either

$$\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p} \text{ or } \left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}.$$

(vi) If p is prime and $0 \leq k \leq p-1$, then

$$k!(p-k-1)! \equiv (-1)^{k+1} \pmod{p}.$$

(vii) If p and q are distinct primes, then for any integer a,

$$pq \mid a^{pq} - a^p - a^q + a.$$

(viii) If p and $p+2$ are twin primes, then

$$4((p-1)! + 1) + p \equiv 0 \pmod{p(p+2)}.$$