MTH 305: Practice assignment 7

1 Primitive roots

Establish the following assertions.

(i) If $|a|_p = 2k$, where p is a prime, then $a^k \equiv -1 \pmod{p}$.

(ii) If $|a|_n = n - 1$, then n is a prime.

(iii) $\phi(2^n - 1)$ is a multiple of n, for each $n > 1$.

(iv) If $|a|_p = 3$, where p is an odd prime, then $|a+1|_p = 6$.

(v) The odd prime divisors of $n^4 + 1$ are of the form $8k + 1$.

(vi) If p and q are odd primes and $q \mid a^p - 1$, then either $q \mid a - 1$ or $q = 2kp + 1$, for some integer k.

(vii) There are infinitely many primes of the form $6k + 1$ and $8k + 1$.

(viii) If r is a primitive root of n, then r^k is a primitive root of n if and only if $\gcd(k, \phi(n)) = 1$.

(ix) If p is an odd prime, then $\sum_{k=0}^{p-2} x^k \equiv 0 \pmod{p}$ has exactly $p - 2$ incongruent solutions.

(x) Let r be a primitive root of an odd prime p.

  (a) $r^{(p-1)/2} \equiv -1 \pmod{p}$.

  (b) If r' is a another primitive root of p, then rr' is not a primitive root of p.

  (c) If $p \equiv 1 \pmod{4}$, then $-r$ is also a primitive root of p.

(d) If $p \equiv 3 \pmod 4$, then $|-r|_p = (p-1)/2$.

(xi) Let p be an odd prime. Then:

(a) The product of the primitive roots of p is congruent to $(-1)^{\phi(p-1)}$ modulo p.

(b)
$$\sum_{k=0}^{p-2} r^{kn} \equiv \begin{cases} 0 \pmod p, & \text{if } (p-1) \nmid n, \text{ and} \\ -1 \pmod p, & \text{if } (p-1) \mid n. \end{cases}$$

(c) Any primitive root r of p^n is also a primitive root of p.

(d) A primitive root r of p^k is a primitive of $2p^k$ if and only if r is an odd integer.

(e) When r is a primitive root of p such that $(r+tp)^{p-1} \not\equiv 1 \pmod{p^2}$, we have $r + tp$ is a primitive root of p^k, for each $k \geq 1$.

2 Theory of indices

(i) Establish the following assertions.

(a) Let r be a primitive root of an odd prime p. Then:

(1) When r' is also a primitive root of p, we have

$$\operatorname{ind}_{r'} a = (\operatorname{ind}_r a)(\operatorname{ind}_{r'} r) \pmod{p-1}.$$

(2) $\operatorname{ind}_r(-1) = \operatorname{ind}_r(p-1) = \frac{1}{2}(p-1)$.

(3) $\operatorname{ind}_r(p-a) \equiv \operatorname{ind}_r a + \frac{p-1}{2} \pmod{p-1}$.

(4) The congruence $a^x \equiv b \pmod p$ has a solution if and only if $d \mid \operatorname{ind}_r b$, where $d = \gcd(\operatorname{ind}_r a, p-1)$. In this case, there are d incongruent solutions modulo $p-1$.

(b) Let p be an odd prime. Then:

(1) $x^2 \equiv -1 \pmod p$ is solvable if and only if $p \equiv 1 \pmod 4$.

(2) $x^4 \equiv -1 \pmod p$ is solvable if and only if $p \equiv 1 \pmod 8$.

(ii) Solve the following congruences, after determining whether they are solvable.

(a) $x^8 \equiv 10 \pmod{11}$.

(b) $8x^5 \equiv 10 \pmod{17}$.

(c) $x^3 \equiv 3 \pmod{19}$

(d) $x^5 = 13 \pmod{23}$

(e) $x^7 \equiv 15 \pmod{29}$

(f) $5^x \equiv 4 \pmod{19}$.