

MATH567 Abstract Algebra II : Solutions to Sec. 13.6, exercises 14–17.

14. Suppose p_1, p_2, \dots, p_k are the only primes dividing the values $P(n)$, $n = 1, 2, \dots$. Since $P(x)$ is monic of degree at least one, there exists a positive integer N such that $a := P(N)$ is non-zero. Now if

$$P(x) = x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0$$

then

$$\begin{aligned} & P(N + ap_1p_2 \cdots p_kx) \\ &= (N + ap_1p_2 \cdots p_kx)^m + a_{m-1}(N + ap_1p_2 \cdots p_kx)^{m-1} + \dots + a_1(N + ap_1p_2 \cdots p_kx) + a_0 \\ &= N^m + a_{m-1}N^{m-1} + \dots + a_1N + a_0 + ap_1p_2 \cdots p_k\rho(x) \\ &= a + ap_1p_2 \cdots p_k\rho(x) \end{aligned}$$

for some polynomial $\rho(x) \in \mathbb{Z}[x]$. Therefore

$$Q(x) = a^{-1}P(N + ap_1p_2 \cdots p_kx) = 1 + p_1p_2 \cdots p_k\rho(x)$$

is an element of $\mathbb{Z}[x]$ and moreover

$$Q(n) = 1 + p_1p_2 \cdots p_k\rho(n) \equiv 1 \pmod{p_1p_2 \cdots p_k}$$

for $n = 1, 2, \dots$. In particular, $Q(n)$ is never divisible by p_1, p_2, \dots , or p_k . For n sufficiently large (to ensure that $Q(n) > 1$), $Q(n)$ will have a prime factor different to p_1, p_2, \dots, p_k . Therefore

$$P(N + ap_1p_2 \cdots p_kn) = aQ(n)$$

will also have a prime factor different to p_1, p_2, \dots, p_k . This contradiction shows that there must be infinitely many distinct prime divisors of

$$P(1), P(2), P(3), \dots$$

15. Suppose that $p|a$. Then $\Phi_m(a) \equiv \Phi_m(0) \pmod{p}$, since $\Phi_m(x)$ has integer coefficients. But $\Phi_m(0)$ is the constant term of $\Phi_m(x)$; up to ± 1 , it is the product of the primitive m th roots of unity. These all lie on the unit circle in \mathbb{C} , and hence so does their product. Since $\Phi_m(0)$ is an integer, it must be ± 1 . So if $\Phi_m(a) \equiv 0 \pmod{p}$, then p cannot divide a , and a is relatively prime to p .

Substituting $x = a$ into

$$x^m - 1 = \prod_{d|m} \Phi_d(x)$$

and using $\Phi_m(a) \equiv 0 \pmod{p}$ shows that $a^m - 1 \equiv 0 \pmod{p}$. Therefore the order of a divides m .

Suppose that $a^d - 1 \equiv 0 \pmod{p}$ for some divisor d of m , with $d < m$. Then

$$a^d - 1 = \prod_{d'|d} \Phi_{d'}(a) \equiv 0 \pmod{p}$$

so $\Phi_{d'}(a) \equiv 0 \pmod{p}$ for some $d' \leq d < m$. Therefore $x^m - 1$ would have a as a repeated root (mod p), since it is a root of both the factor $\Phi_m(x)$ and the factor $\Phi_{d'}(x)$. But this is impossible: recall that

$$D_x(x^m - 1) = mx^{m-1}$$

has only zero as a root, so $x^m - 1$ is separable over \mathbb{F}_p , meaning it has no repeated roots. Therefore the order of a in $(\mathbb{Z}/p\mathbb{Z})^\times$ is precisely m .

16. Suppose that p does not divide m . By exercise 15 (since $\Phi_m(a) \equiv 0 \pmod{p}$), a must be relatively prime to p and the order of a in $(\mathbb{Z}/p\mathbb{Z})^\times$ must be precisely m . The order of the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is $p - 1$, so the order of the element a must divide $p - 1$, i.e., $m | p - 1$. Therefore $p \equiv 1 \pmod{m}$.

17. Firstly, because $\Phi_m(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree at least one, then exercise 14 shows that there are infinitely many prime divisors of the integers

$$\Phi_m(1), \Phi_m(2), \Phi_m(3), \dots$$

(and hence infinitely many odd prime divisors). By exercise 16, each of these odd prime divisors must either divide m or be congruent to 1 (mod m). Since m can only have finitely many prime divisors, there must be infinitely many primes congruent to 1 (mod m).