

Math 4150 Practice Midterm 2 Solutions

Problem 3 Let $r = e_n(a)$, $s = e_n(b)$, $k = e_n(ab)$. We have $(ab)^{rs} = (a^r)^s (b^s)^r = 1 \cdot 1 = 1$, so $k|rs$. Moreover, $(ab)^k = 1$, and raising to the s -th power we get $a^{ks} b^{sk} = 1$, hence $a^{ks} = 1$ and $r|sk$. Since $(r, s) = 1$, then $r|k$. Similarly, $s|k$ and therefore $rs|k$. We conclude that $k = rs$.

Problem 4 See solutions to homework 6, problem 4.

Problem 6(a) Let $r = e_n(a)$. We claim that $r = n - 1$. Since $a^{n-1} \equiv 1 \pmod{n}$, then $r|n - 1$. Suppose $r < n - 1$. Then r divides $\frac{n-1}{q}$ for some prime q dividing $n - 1$. In particular, $a^{\frac{n-1}{q}} \equiv 1 \pmod{n}$, which is a contradiction. Thus $r = n - 1$. Now, by Euler's theorem, $r|\phi(n)$, so $n - 1$ divides $\phi(n)$. In particular $n - 1 \leq \phi(n)$, and this implies n is prime (since it means there are at least $n - 1$ numbers between 1 and n which are relatively prime to n). Moreover, since $e_n(a) = n - 1$, then a is a primitive root modulo n .

Problem 9 Let p be a prime dividing n and let a be a primitive root modulo p . Since $a^n \equiv a \pmod{n}$, then in particular $a^n \equiv a \pmod{p}$, so $a^{n-1} \equiv 1 \pmod{p}$. Therefore the order of a modulo p , which is $p - 1$, divides $n - 1$.

Problem 10 The index of $p - 1$ modulo p is the unique exponent k between 1 and $p - 1$ such that $g^k = p - 1$, that is, $g^k = -1$. Since $g^{p-1} = 1$, then $(g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) = 0$. Since the order of g is $p - 1$, then $g^{\frac{p-1}{2}} \neq 1$, so we must have $g^{\frac{p-1}{2}} = -1$. Hence, the index of $p - 1$ modulo p is $\frac{p-1}{2}$.

Problem 11 See solutions to homework 6, problem 8.

Problem 12 Let r be the order of $-g$ modulo p . Since $p - 1$ is even, we have $(-g)^{p-1} = g^{p-1}$, which is 1 modulo p . Therefore $r|p - 1$. Suppose r is odd. Then r divides $\frac{p-1}{2}$, so $(-g)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. However, since $\frac{p-1}{2}$ is even, this implies $g^{\frac{p-1}{2}} = (-g)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. This contradicts the fact that the

order of g is $p - 1$. Therefore r must be even, so $g^r = (-g)^r \equiv 1 \pmod{p}$. Thus the order of g , which is $p - 1$, divides r , and we conclude $r = p - 1$. Hence, $-g$ is a primitive root modulo p .

Problem 13 Let a be any integer relatively prime to n . We claim that $a^{\phi(n)/2} \equiv 1 \pmod{n}$. This will imply that the order of a modulo n is less than $\phi(n)$, so a is not a primitive root modulo n . Write $n = p^c q^d t$ where t is not divisible by p or q . Then $\phi(n) = \phi(p^c)\phi(q^d)\phi(t)$. Note that since p and q are odd, then $\phi(p^c)$ and $\phi(q^d)$ are even. We have

$$a^{\phi(n)/2} = (a^{\phi(p^c)})^{\frac{\phi(q^d)}{2}\phi(t)},$$

and by Euler's theorem, $a^{\phi(p^c)} \equiv 1 \pmod{p^c}$. Therefore $a^{\phi(n)/2} \equiv 1 \pmod{p^c}$. A similar argument shows that $a^{\phi(n)/2} \equiv 1 \pmod{q^d}$ and $a^{\phi(n)/2} \equiv 1 \pmod{t}$. By the chinese remainder theorem, $a^{\phi(n)/2} \equiv 1 \pmod{n}$, as claimed.

Problem 14 Let $d = (p - 1, k)$ and let r be the order of g^k modulo p . Note that $(g^k)^{\frac{p-1}{d}} = (g^{p-1})^{\frac{k}{d}} = 1$, so r divides $\frac{p-1}{d}$. Moreover, we have $(g^k)^r = 1$, so $g^{kr} = 1$, so $p - 1$ divides kr . Then $\frac{p-1}{d}$ divides $\frac{k}{d}r$. Since $\frac{p-1}{d}$ and $\frac{k}{d}$ are relatively prime, then $\frac{p-1}{d}$ divides r . Thus we have shown that the order of g^k is $\frac{p-1}{(p-1, k)}$. In particular, g^k is a primitive root if and only if $(p - 1, k) = 1$.

Problem 17 You know $\phi(n) = (p - 1)(q - 1) = pq - p - q + 1 = n - p - q + 1$, so $p + q = n + 1 - \phi(n)$ is known. Thus for the numbers p and q , you know their sum, $n + 1 - \phi(n)$, and their product, n . Then it is a simple exercise to solve a quadratic equation whose solution is p , or q . This is because a system $x + y = a$, $xy = b$ can be solved by substituting $y = b/x$ into the first equation and solving a quadratic equation.

Problem 20 See the solution to homework 7, problem 25.6.

Problem 22(b) Note that p divides $n^2 + 1$ if and only if $n^2 \equiv -1 \pmod{p}$. Thus, to show that p cannot divide $n^2 + 1$, it suffices to show that -1 is not a quadratic residue modulo p . This follows immediately from quadratic reciprocity: $\left(\frac{-1}{p}\right) = -1$ since $p \equiv 3 \pmod{4}$.

Problem 23

(a) See solutions to homework 7, problem 24.6.

(b) Note that q divides $2^p - 1$ if and only if $2^p \equiv 1 \pmod{q}$, that is, $2^{\frac{q-1}{2}} \equiv 1 \pmod{q}$. By Euler's criterion, this is equivalent to $\left(\frac{2}{q}\right) = 1$, and this follows from quadratic reciprocity since $q \equiv 7 \pmod{8}$.

Problem 24 Pepin's test states that F_m is prime if and only if $3^{\frac{F_m-1}{2}} \equiv -1 \pmod{F_m}$.

Problem 25 Suppose $q = 1729$ is prime. Note that $864 = \frac{q-1}{2}$. By Euler's criterion, $11^{864} \equiv \left(\frac{11}{q}\right) \pmod{q}$, so $\left(\frac{11}{q}\right) = 1$. However, by quadratic reciprocity we have $\left(\frac{11}{q}\right) = \left(\frac{q}{11}\right) = \left(\frac{2}{11}\right) = -1$. Therefore, 1729 is not prime.