

PRACTICE FINAL SOLUTIONS, MATH 441

NIGEL BOSTON

1. (i) The gcd of 10 and 21 is 1. (ii) $1 = 21 - 2 * 10$, so $10(-2) \equiv 1 \pmod{21}$, so -2 is a solution (as is 19 etc.) (iii) The order of 10 equals the order of its inverse -2 . The powers of $-2 \pmod{21}$ are $-2, 4, -8, 16, -11, 1$ so the order is 6.

2. (i) If $n = md$ and $x = 2^m$, then $2^n - 1 = 2^{md} - 1 = x^d - 1$, which is divisible by $x - 1$. (ii) If n isn't prime, say has proper factor m , then $2^n - 1$ is divisible by $2^m - 1$ so isn't prime. (iii) Since n is prime, it must be the order of $2 \pmod{p}$. By Fermat, n divides $p - 1$ i.e. $p \equiv 1 \pmod{n}$. (iv) The smallest prime that is $1 \pmod{11}$ is 23 and by division we find that $2^{11} - 1 = 23 * 89$.

3. (i) We're given that p divides $10^d - 1$, i.e. $(10^d - 1)/p$ is an integer. Thus $10^d/p$ and $1/p$ differ by an integer, so have the same decimal part, so the decimal expansion of $1/p$ has period d . (ii) The order d divides $p - 1$ by Fermat. (iii) If the period is 3, then p divides $10^3 - 1 = 999 = 3^3 * 37$. 37 does not divide $10^1 - 1$, so the period is exactly 3 for $p = 37$.

4. (i) $\phi(20) = \phi(5)\phi(4) = 4 * 2 = 8$. (ii) The powers of 3 $\pmod{20}$ are 3, 9, 7, 1 so the order is 4. (iii) The subgroup itself is $\{[3], [9], [7], [1]\}$. $8/4 = 2$ so there's just one other coset, which must be everything else in U_{20} , namely $\{[11], [13], [17], [19]\}$. (iv) Lagrange says that the number of cosets equals the order of the group divided by the order of the subgroup, namely $2 = 8/4$.

5. (i) Let $m(t)$ be any irreducible polynomial of degree 3 over \mathbf{F}_2 , such as $t^3 + t + 1$. Then $\mathbf{F}_2[t]/(t^3 + t + 1)$ works. (ii) The order of a divides $8 - 1 = 7$. Since $a \neq 1$, the order isn't 1, so it's 7, and so a is primitive. (iii) Every element of F satisfies $x^8 = x$ and so $x^8 - x$ has 8 distinct linear factors $x - a$ as a runs over F . But then $x^8 - x = \prod_F (x - a)$.