

FINAL SOLUTIONS, MATH 441

NIGEL BOSTON

1. (i) Powers of 2 (mod 12) go 2, 4, 8, 4, 8, 4, ... Since 101 is odd, we get 8. (ii) $99^{101} \equiv (-1)^{101} \equiv -1 \pmod{100}$ (iii) $121212121 \equiv 1+2+1+2+1+2+1+2+1 \equiv 4 \pmod{9}$. (iv) $121212121 \equiv 21 + 21 * 100 + 21 * 100^2 + 21 * 100^3 + 100^4 \equiv 21 - 21 + 21 - 21 + 1 \equiv 1 \pmod{101}$

2. (i) If $k = md$ and $x = 2^d$, then $2^k + 1 = 2^{md} + 1 = x^m + 1$, which is divisible by $x + 1 = 2^d + 1$ since m is odd (use the root test). (ii) If k is not a power of 2, then it has an odd factor m and then $2^k + 1$ is divisible by $2^d + 1$, so $2^k + 1$ is not prime. (iii) The hint holds since $(F_{n-1} - 1)^2 = (2^{2^n})^2 = 2^{2^{n+1}}$. The claim is true for $n = 1$ since $F_1 = 5 = F_0 + 2$. Assume the claim is true for a particular n , i.e. that $F_0 F_1 \dots F_{n-1} + 2 = F_n$. Then $F_0 F_1 \dots F_n = F_0 F_1 \dots F_{n-1} F_n = (F_n - 2) F_n = (F_n - 1)^2 - 1 = F_{n+1} - 2$ by the hint, implying that the claim is true with n replaced by $n + 1$. This completes the induction. (iv) Suppose $m < n$. If p is a common factor of F_m and F_n , then by (iii) p divides $F_n - F_0 F_1 \dots F_{n-1} = 2$. But any factor of F_m must be odd. So F_m and F_n have no common factor, other than 1. This implies there are infinitely many primes since F_n must be divisible by some prime that hasn't appeared in the factorizations of F_0, F_1, \dots, F_{n-1} .

3. (i) We need an element of order 4 in U_{17} . Looking at powers of 2, we get 2, 4, 8, -1, so 2 will have order 8 so $2^2 = 4$ has order 4. Then $H = \{[4], [-1], [-4], [1]\} = \{[4], [16], [13], [1]\}$. (ii) If H is a subgroup of the finite group G , then the order of G divided by the order of H is an integer, namely the number of cosets of H in G . (iii) For the cosets, $H = \{[4], [16], [13], [1]\}$, $2 * H = \{[[8], [15], [9], [2]]\}$, $3 * H = \{[12], [14], [5], [3]\}$, leaving as the remaining coset $\{[6], [7], [10], [11]\}$. (iv) By Cayley, we just look at the effect of multiplication by the elements of H . Multiplication by [1] maps [1], [4], [-1], [-4] to [1], [4], [-1], [-4]. Multiplication by [4] maps [1], [4], [-1], [-4] to [4], [-1], [-4], [1]. Multiplication by [-1] maps it to [-1], [-4], [1], [4]. Multiplication by [-4] maps it to [-4], [1], [4], [-1]. Relabeling, the homomorphism is [1] \mapsto (1, 2, 3, 4), [4] \mapsto (2, 3, 4, 1), [-1] \mapsto (3, 4, 1, 2), [-4] \mapsto (4, 1, 2, 3).

4. (i) $x^4 + 2 = x(x^3 + x + 1) + (2x^2 + 2x + 2)$, $x^3 + x + 1 = (2x + 1)(2x^2 + 2x + 2) + (x + 2)$, $2x^2 + 2x + 2 = (2x + 1)(x + 2) + 0$. So a greatest common divisor is $x + 2$. (ii) $x + 2 = (x^3 + x + 1) - (2x + 1)(2x^2 + 2x + 2) = (x^3 + x + 1) - (2x + 1)((x^4 + 2) - x(x^3 + x + 1)) = (1 + x + 2x^2)(x^3 + x + 1) - (2x + 1)(x^4 + 2)$. (iii) $\mathbf{F}_3[\alpha]$ has $3^3 = 27$ elements. (iv) $x^3 + x + 1 = (x + 2)(x^2 + x + 2)$, where $x^2 + x + 2$ is irreducible (since it has no root). So $\alpha + 2, \alpha^2 + \alpha + 2$ are zero divisors, as is say $2\alpha + 1$ (or any multiple of either of the factors of $x^3 + x + 1$). As for units, we need elements relatively prime to the factors of $x^3 + x + 1$, so e.g. $1, 2, \alpha, \alpha^2, \dots$