

1. For more detailed solutions to problems like these, see the homework assignments and lecture notes.

- (a) By Euclid,  $\gcd(688, 164) = 4$  and  $-5 \cdot 688 + 21 \cdot 164 = 4$ .
  - (b) By Fermat,  $7^{29} \equiv 7$  and by Wilson  $28! \equiv -1 \pmod{29}$ , so  $7^{29} \cdot 28! \equiv -7 \pmod{29}$ , meaning the remainder is 22.
  - (c)  $\varphi(121) = \varphi(11^2) = (11^2 - 11) = 110$  and  $\varphi(5^3 7^5) = (5^3 - 5^2)(7^5 - 7^4)$ .
  - (d) If  $x = 0.1\overline{49}$  then  $990x = 1000x - 10x = 149.\overline{49} - 1.\overline{49} = 148$ , so  $x = 148/990$ .
  - (e) Units are  $\{1, 5, 7, 11\}$ , zero divisors are  $\{2, 3, 4, 6, 8, 9, 10\}$ .
  - (f) By Euclid,  $39 \cdot 5 - 2 \cdot 97 = 1$  so  $5^{-1} \equiv 39$ , and  $14 \cdot 7 - 1 \cdot 97 = 1$  so  $7^{-1} \equiv 14$ .
  - (g) Note  $\varphi(22) = 10$  so orders divide 10. Testing  $3^5 \equiv 3^4 \cdot 3^1 \equiv (-7)(3) \equiv 1$  shows 3 has order 5. Likewise testing  $7^2 \equiv 5$  and  $7^5 \equiv 7^4 \cdot 7^1 \equiv 3 \cdot 7 \equiv -1$  shows 7 has order 10.
  - (h) Plug in  $n = 7 + 14a$  to  $n \equiv 2 \pmod{9}$  to get  $n \equiv 119 \pmod{126}$ .
  - (i) Testing squares above 851 yields  $30^2 - 851 = 49 = 7^2$ , so  $851 = (30 - 7)(30 + 7) = 23 \cdot 37$ .
  - (j) By Euclid,  $\gcd = x + 1$  and  $1(x^3 + 1) + (2x)(x^2 + 1) = 1$ .
  - (k) By Euclid,  $\gcd = -4 - i$  and  $(1)(11 + 24i) + (-1 - 2i)(13 - i) = -4 - i$ .
  - (l) By Euclid,  $1(x^3 + 5) - (x^2 - 3x + 9)(x + 3) = -22$  so  $(x + 3)^{-1} = -(x^2 - 3x + 9)/22$ .
  - (m) Inverse of  $1 + i$  is  $-4 + 3i$  so solution is  $n \equiv 3(-4 + 3i) \pmod{8 + i}$ .
  - (n) Units are  $\overline{1}, \overline{2}, \overline{x + 1}, \overline{2x + 2}$ ; zero divisors are  $\overline{x}, \overline{x + 2}, \overline{2x}, \overline{2x + 1}$ .
  - (o) For  $m = 1, 2, 4, p^d, 2p^d$  it is  $\varphi(\varphi(m))$ , otherwise it is 0: 17 has 4, 18 has 2, 19 has 6, 20 has 0, 21 has 0.
  - (p) For  $7 + 2i$  it is  $N(7 + 2i) = 53$  and for  $\mathbb{F}_5[x] \pmod{x^4 + 2}$  it is  $5^4 = 625$ .
  - (q)  $x^2 + x + 1$  is  $(x - 1)^2$  in  $\mathbb{F}_3[x]$ , irreducible in  $\mathbb{F}_5[x]$ , and  $(x - 2)(x - 4)$  in  $\mathbb{F}_7[x]$ .
  - (r)  $(5^5 - 5)/3 = 40$  of degree 3,  $(5^4 - 5^2)/4 = 150$  of degree 4,  $(5^5 - 5)/5 = 624$  of degree 5.
  - (s) By factoring the norms, we see  $51 = 3(4 + i)(4 - i)$  and  $-3 + 11i = (1 + i)(1 + 2i)(3 + 2i)$ .
  - (t) By Fermat's theorem,  $104 = 10^2 + 2^2$  and  $666 = 21^2 + 15^2$  can, 224 and 420 cannot.
  - (u) Since  $N(1 + i) = 2$ ,  $N(3) = 3^2$ ,  $N(2 \pm i) = 5$ , take  $(1 + i)3(2 + i)^2 = 21 - 3i$  yielding  $450 = 21^2 + 3^2$ , and also  $(1 + i)3(2 + i)(2 - i) = 15 + 15i$  yielding  $450 = 15^2 + 15^2$ .
  - (v) For leg 29 need  $k(s + t)(s - t) = 29$  yielding  $k = 1$ ,  $s + t = 29$ ,  $s - t = 1$  so  $(k, s, t) = (1, 15, 14)$  giving 29-420-421. For hypotenuse 29 need  $k(s^2 + t^2) = 29$  so  $(k, s, t) = (1, 5, 2)$  giving 20-21-29.
  - (w) Compute  $\left(\frac{13}{2027}\right) = \left(\frac{2027}{13}\right) = \left(\frac{-1}{13}\right) = 1$  and  $\left(\frac{26}{2027}\right) = \left(\frac{2}{2027}\right) \left(\frac{13}{2027}\right) = (-1)(1) = -1$  since  $\left(\frac{2}{p}\right) = -1$  for  $p \equiv 3, 5 \pmod{8}$ . So 13 is a QR but 26 is not.
  - (x) Compute  $\left(\frac{28}{71}\right) = \left(\frac{2}{71}\right)^2 \left(\frac{7}{71}\right) = 1 \cdot - \left(\frac{71}{7}\right) = - \left(\frac{1}{7}\right) = -1$  and  $\left(\frac{15}{71}\right) = - \left(\frac{71}{15}\right) = - \left(\frac{11}{15}\right) = \left(\frac{15}{11}\right) = \left(\frac{4}{11}\right) = 1$  using reciprocity for Jacobi symbols. So 15 is a QR but 28 is not.
  - (y) We compute  $\left(\frac{103}{307}\right) = - \left(\frac{307}{103}\right) = - \left(\frac{-2}{131}\right) = 1$  since  $\left(\frac{-2}{p}\right) = -1$  for  $p \equiv 5, 7 \pmod{8}$ , and  $\left(\frac{141}{307}\right) = \left(\frac{307}{141}\right) = \left(\frac{25}{141}\right) = 1$ .
  - (z) We compute  $\left(\frac{47}{245}\right) = \left(\frac{245}{47}\right) = \left(\frac{10}{47}\right) = \left(\frac{2}{47}\right) \left(\frac{5}{47}\right) = 1 \cdot \left(\frac{47}{5}\right) = 1 \cdot \left(\frac{2}{5}\right) = -1$  since  $\left(\frac{2}{p}\right) = 1$  for  $p \equiv 1, 7 \pmod{8}$ , and  $\left(\frac{177}{245}\right) = \left(\frac{245}{177}\right) = \left(\frac{68}{177}\right) = \left(\frac{2}{177}\right)^2 \left(\frac{17}{177}\right) = \left(\frac{177}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1$ .
-

2. Additional details can be found in the lecture notes.

- (a) Finding the four decodings of a single Rabin ciphertext  $c$  does allow rapid factorization of the modulus: if the decodings are  $\pm m$  and  $\pm w$  then  $\gcd(m+w, N)$  will be one of the prime factors of  $N$ . If Eve is able to obtain the four decodings of any single ciphertext, she can factor  $N$ : for this reason Rabin encryption is not suitable for modern use.
  - (b) Using a zero-knowledge protocol like the Rabin protocol described in class, where Peggy proves to an arbitrarily high probability that she knows the square root of a particular value  $s^2$  modulo  $N = pq$ , will allow Peggy to convince Victor that she knows the secret  $s$  without revealing any information that makes  $s$  easily calculable.
  - (c) Using primality/compositeness tests like Miller-Rabin and Solovay-Strassen allow for rapid and accurate testing of primality even for very large integers.
  - (d) If a polynomial's irreducible factorization has no linear terms then it will have no roots, but the factorization could still be nontrivial. For example,  $q(x) = x^4 + 3x^2 + 2 = (x^2 + 1)(x^2 + 2)$  in  $\mathbb{R}[x]$  has no real roots, but still factors nontrivially.
  - (e) We can use quadratic reciprocity to calculate the Legendre symbol  $\left(\frac{3}{11291867}\right) = -\left(\frac{11291867}{3}\right) = -\left(\frac{2}{3}\right) = +1$ , so in fact there is a solution.
  - (f) We can use Berlekamp's root-finding algorithm to solve  $q(x) \equiv 0 \pmod{p}$  much more quickly than using a brute-force search: by computing  $\gcd(x^{(p-1)/2} - 1, q(x-a))$  using successive squaring and the Euclidean algorithm, if  $q$  has a root then each value of  $a$  we try has at least a 50% chance of yielding a partial factorization. This procedure is very efficient even for large  $p$ .
  - (g) This is an application of the Solovay-Strassen test: if  $\left(\frac{a}{m}\right) \neq a^{(m-1)/2} \pmod{m}$  then  $m$  must be composite.
- 

3. Many problems of similar types were covered on the homework.

- (a) Induct on  $n$  with base case  $n = 1$ . Inductive step: If  $1 + \frac{1}{2} + \frac{1}{4} + \dots + \frac{1}{2^n} = 2 - \frac{1}{2^n}$ , then  $1 + \frac{1}{2} + \frac{1}{4} + \dots + \frac{1}{2^n} + \frac{1}{2^{n+1}} = 2 - \frac{1}{2^n} + \frac{1}{2^{n+1}} = 2 - \frac{1}{2^{n+1}}$  as required.
- (b) Induct on  $n$  with base cases  $n = 0, 1$ . Inductive step: if  $c_n = (6-2n)2^n$  and  $c_{n-1} = (6-2(n-1))2^{n-1} = (4-n)2^n$  then  $c_{n+1} = 4(6-2n)2^n - 4(4-n)2^n = (24-8n-16+4n)2^n = (6-2(n+1))2^{n+1}$  as required.
- (c) Note  $\varphi(18) = 6$ . Then  $5^6 \equiv 1 \pmod{18}$  by Euler, but  $5^2 \equiv 7$  and  $5^3 \equiv -1 \pmod{18}$ , so order does not divide 2 or 3, hence must be 6.
- (d) Note  $3^4 \equiv 81 \equiv 8$  so  $3^8 \equiv 8^2 \equiv 64 \equiv -9$ . Then  $3^{12} \equiv 3^8 3^4 \equiv 8 \cdot (-9) \equiv 1 \pmod{73}$  so the order divides 12. But  $3^4 \equiv 8$  and  $3^6 \equiv 3^4 3^2 \equiv 8 \cdot 9 \equiv -1$ : hence the order does not divide 6 or 4, so it must be 12.
- (e) By Euler,  $a^4 \equiv 1 \pmod{5}$  for every unit, and  $0^4 \equiv 0 \pmod{5}$ . Then the sum of three fourth powers is 0, 1, 2, or 3 mod 5, hence cannot be 2024 since 2024 is 4 mod 5.
- (f) If  $p \leq 100$  is prime then  $p|99!$  so  $p$  does not divide  $99! - 1$ . By Wilson's theorem,  $99! \equiv 100!/100 \equiv 100/100 \equiv 1 \pmod{101}$ , so 101 does divide  $99! - 1$ .
- (g) For  $q(x) = x^3 + 4x + 2$  modulo 5, we have  $q(0) = 2, q(1) = 2, q(2) = 3, q(3) = 1, q(4) = 2$  so  $q$  has no roots in  $\mathbb{F}_5$ . Since  $q$  has degree 3 this means it is irreducible in  $\mathbb{F}_5[x]$ , meaning  $\mathbb{F}_5[x]$  modulo  $q$  is a field.
- (h) For  $q(x) = x^3 + 4x + 2$  modulo 7, we have  $q(1) = 0 \pmod{7}$  so  $q$  has a root  $x = 1$ . This means  $q$  is reducible modulo 7 so  $\mathbb{F}_7[x]$  modulo  $q$  is not a field. In fact,  $q(x) = (x-1)^2(x-5) \pmod{7}$ .
- (i) Since  $N(a + b\sqrt{26}) = a^2 - 26b^2$  it suffices to decide whether  $a^2 - 26b^2 = \pm 2$  has any solutions. Reducing both sides mod 13 yields  $a^2 \equiv \pm 2 \pmod{13}$ , but since  $\left(\frac{2}{13}\right) = \left(\frac{-2}{13}\right) = -1$  since  $13 \equiv 5 \pmod{8}$ , there are no solutions to this congruence. Therefore there are no elements of norm 2 or -2.
- (j) If we had a factorization  $2 + \sqrt{26} = bc$  then  $N(b)N(c) = N(bc) = N(2 + \sqrt{26}) = -22$ . But  $N(b), N(c)$  cannot equal  $\pm 2$  by (g), so the only possible values would have one of  $N(b), N(c)$  equal to  $\pm 1$  hence  $b$  or  $c$  would be a unit. Thus  $2 + \sqrt{26}$  is irreducible. But  $(2 + \sqrt{26})|(-2) \cdot (11)$  since  $-22 = N(2 + \sqrt{26}) = (2 + \sqrt{26})(2 - \sqrt{26})$ , but  $2 + \sqrt{26}$  does not divide -2 or 11 since its norm -22 does not divide  $N(-2) = 4$  or  $N(11) = 121$ . Thus  $2 + \sqrt{26}$  is not prime.

- (k) It is not hard to list all the units to see that there are 4: 1, 2,  $x + 2$ , and  $2x + 1$ . Then  $\overline{x + 2}^2 \equiv \overline{x^2 + 4x + 4} \equiv 1$  so  $\overline{x + 2}^4 \equiv 1$  as well.
- (l) Since  $x^3 + x + 1$  has no roots in  $\mathbb{F}_2$  and has degree 3, it is irreducible. Then  $\mathbb{F}_2[x]$  modulo  $x^3 + x + 1$  is a field with 8 elements hence 7 units. By Euler's theorem every element's order divides 7, so since the order of  $x$  is not 1, it must be 7, so it is a primitive root.
- (m) Compute  $\left(\frac{11}{97}\right) = \left(\frac{97}{11}\right) = \left(\frac{-2}{11}\right) = +1$  since  $11 \equiv 3 \pmod{8}$ . Since 97 is prime, the Legendre symbol being +1 means 11 is a quadratic residue.
- (n) Completing the square by adding 9 gives  $(x + 3)^2 \equiv 23 \pmod{101}$ . (Alternatively, the quadratic formula says to compute  $\sqrt{23}$ .) We have  $\left(\frac{23}{101}\right) = \left(\frac{101}{23}\right) = \left(\frac{9}{23}\right) = +1$  so 23 is a quadratic residue modulo 101 hence there is a solution to  $(x + 3)^2 \equiv 23 \pmod{101}$ .
- (o) We want to compute  $\left(\frac{3}{p}\right)$ . If  $p \equiv 1 \pmod{4}$ , then  $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = +1$  only when  $p \equiv 1 \pmod{3}$  which together say  $p \equiv 1 \pmod{12}$ . Likewise, if  $p \equiv 3 \pmod{4}$ , then  $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = +1$  only when  $p \equiv 2 \pmod{3}$ , which together say  $p \equiv 11 \pmod{12}$ . If  $p \equiv 5, 7 \pmod{12}$  then the calculations show  $\left(\frac{3}{p}\right) = -1$ .
- (p) We want to compute  $\left(\frac{-3}{p}\right)$ . If  $p \equiv 1 \pmod{4}$ , then  $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = +1 \cdot \left(\frac{p}{3}\right) = +1$  only when  $p \equiv 1 \pmod{3}$ . Likewise, if  $p \equiv 3 \pmod{4}$ , then  $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = -1 \cdot -\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = +1$  only when  $p \equiv 1 \pmod{3}$ . So in either case,  $\left(\frac{-3}{p}\right) = +1$  only when  $p \equiv 1 \pmod{3}$ .
- (q) Completing the square gives  $n^2 + 4n - 1 = (n + 2)^2 - 5$ , so we want primes  $p$  such that there is a solution to  $(n + 2)^2 \equiv 5 \pmod{p}$ , which is equivalent to solving  $x^2 \equiv 5 \pmod{p}$ . Clearly there is a solution for  $p = 2, 5$ . For other  $p$  we compute  $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$  which is +1 for  $p \equiv 1, 4 \pmod{5}$  and -1 for  $p \equiv 2, 3 \pmod{5}$ . So  $p$  divides some  $n^2 + 4n - 1$  iff  $p = 2, 5$  or  $p \equiv 1, 4 \pmod{5}$ .
- (r) Completing the square gives  $n^2 + 6n + 11 = (n + 3)^2 + 2$ , so we want primes  $p$  such that there is a solution to  $(n + 3)^2 \equiv -2 \pmod{p}$ , which is equivalent to solving  $x^2 \equiv -2 \pmod{p}$ . Clearly there is a solution for  $p = 2$ . For other  $p$  we know  $\left(\frac{-2}{p}\right) = +1$  precisely when  $p \equiv 1, 3 \pmod{8}$ . So  $p$  divides some  $n^2 + 6n + 11$  iff  $p = 2$  or  $p \equiv 1, 3 \pmod{8}$ .
-