http://dx.doi.org/10.1090/stml/068/11

Appendix

Answers and Hints for Exercises

Introduction

In this appendix we give answers to some exercises and hints for some other ones.

A.1. Chapter 1

Answers and hints for exercises in Chapter 1.

1.3. The period length of 1/9091 is 10 and that of 1/9901 is 12.

1.4. The period for the decimal expansion of 1/49 is 020408163265306122448979591836734693877551 of length 42.

1.5. The period length of 1/13 in base 3 is 3 because 13 divides $3^3 - 1$.

1.6. The fourth and fifth Mersenne primes are $2^7 - 1$ and $2^{13} - 1$. They give perfect numbers $2^6(2^7 - 1) = 8128$ and $2^{12}(2^{13} - 1) = 33550336$.

A.2. Chapter 2

Answers and hints for exercises in Chapter 2.

2.1. We have $321(19) + 381(-16) = 3$.

2.2. We find that the p_n, $n = 11, 12, 13, \ldots$, are 2801, 11, 17, 5471, 52662739, 23003, 30693651606209, 37, 1741, 1313797957, 887, 71, 7127, 109, 23, 97, 159227, 643679794963466223081509857, ...

2.3. The number is roughly $\ln 10^{300} \approx 691$. It would be half as much if we considered only even 300-digit numbers.

2.4. 99.

2.5. 41.

2.6. 43.

2.8. 0, 1, 4 (mod 8).

2.9. No.

2.11. $-1, +1, +1, -1, +1$.

2.12. Hint: Consider two cases: $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$.

2.13. (a) $10 \equiv 1 \pmod 3$. (b) $10 \equiv -1 \pmod{11}$. (c) $10^2 \equiv -11 \pmod{37}$ and $10^3 \equiv 1 \pmod{37}$.

A.3. Chapter 3

Answers and hints for exercises in Chapter 3.

3.1. The probability that a number near 10^{36} is 10^6-smooth is $\rho(u)$, where $u = 36/6 = 6$, that is, $\rho(6) \approx 0.0000197$. The number of 10^6-smooth numbers between 10^{36} and $10^{36} + 10^7$ is about $10^7\rho(6) \approx 197$.

3.2. Same answer as for the previous exercise.

3.3. Note that $253 = 11 \cdot 23$. The answer is 3 or -3 modulo each of these primes. Combine with four applications of the CRT. The answers are $x = 3, 118, 135, 250$ modulo 253.

3.12. Hint: Use Bang's Theorem 3.19.

3.19. This is Corollary 4.5.

3.20. True, True, True, False.

3.23. Usually not.

A.4. Chapter 4

Answers and hints for exercises in Chapter 4.

4.1. We have $\Phi_5(x) = x^4+x^3+x^2+x+1 = (x^2+3x+1)^2-5x(x+1)^2$, so

$$\Phi_5(5^{5h}) = [5^{2h}+3\cdot 5^h+1-5^{(h+1)/2}(5^h+1)][5^{2h}+3\cdot 5^h+1+5^{(h+1)/2}(5^h+1)].$$

4.2. We have $13^{13h}-1 = (13^h-1)\Phi_{13}(13^h)$ and $\Phi_{13}(13^h) = L_{13h}M_{13h}$, where L_{13h}, M_{13h} are

$$13^{6h} + 7\cdot 13^{5h} + 15\cdot 13^{4h} + 19\cdot 13^{3h} + 15\cdot 13^{2h} + 7\cdot 13^h + 1$$

$$\mp\ 13^{(h+1)/2}(13^{5h} + 3\cdot 13^{4h} + 5\cdot 13^{3h} + 5\cdot 13^{2h} + 3\cdot 13^h + 1).$$

4.17. 14316 is the smallest element of a set of 28 sociable numbers.

4.21. Assume $p < q$. Then $q \mid Q_{q-1}$ but $q \nmid Q_{p-1}$.

4.23. e and d must be relatively prime to $\phi(n)$, which is always even for $n > 2$.

4.26. 193 and 24847873 are the sum of two squares.

A.5. Chapter 5

Answers and hints for exercises in Chapter 5.

5.6. This N is not the sum of two squares because it has a prime factor $3119 \equiv 3 \pmod 4$.

A.6. Chapter 6

Answers and hints for exercises in Chapter 6.

6.3. $p = 1068$.

6.4. Hint: When $N = p^3$, if the CFRAC finds x, y with $x^2 \equiv y^2 \pmod N$ and $1 < \gcd(x-y, N) < N$, then p must be in the factor base.

A.7. Chapter 7

Answers and hints for exercises in Chapter 7.

7.1. Hint: The sum of the roots of the cubic $x^3 + ax + b = 0$ is 0 because there is no x^2 term.

7.2. $2P = (-5, -16)$, $3P = (11, -32)$, $4P = (11, 32)$, $5P = (-5, 16)$, $k = 7$.

7.3. $2P = (0, 0)$, $3P = (2, 7)$, $4P = \infty$, $k = 4$.

A.8. Chapter 8

Answers and hints for exercises in Chapter 8.

8.1. The formula is $p\,\lfloor (I + p - 1)/p \rfloor$.

A.9. Chapter 10

Answers and hints for exercises in Chapter 10.

10.1. One of the prime factors is 576297563010049.

10.5. This is a research problem.

10.6. This is a research problem.

10.7. We tell how to solve the problem in the hint using the solution to the puzzle. Given x and a with $x^2 \equiv a \pmod{N}$, we must find y and b with $y^2 \equiv b \pmod{N}$ and $0 < |b| < |a|$. We may assume that $|a| < N$. Let $R = N/|a|$. Then $R > 1$. The puzzle solution gives k and m with $kR = m^2 + \varepsilon$, where $|\varepsilon| < 1$. Let $y = xm$ and $b = -\varepsilon a$. Then

$$\begin{aligned} y^2 = x^2 m^2 = x^2(kR - \varepsilon) &= x^2 \left(\frac{kN}{|a|} - \varepsilon \right) \\ &\equiv a \left(\frac{kN}{|a|} - \varepsilon \right) = \pm kN - \varepsilon a \equiv -\varepsilon a = b \pmod{N} \end{aligned}$$

and $|b| < |a|$.