Computer Science 1820

Solutions for Recommended Exercises

Section 3.6

---

20. We first express the exponent as the sum of powers of 2:

$$644 \;=\; 512+132 \;=\; 512+128+4.$$

Then, we compute 11 to the power of each power of 2 up to and including 512, reducing each result n modulo 645 by subtracting $\lfloor n/645 \rfloor \cdot 645$ from it:

$11^2 \;\equiv\; 121 \pmod{645}.$

$11^4 \;\equiv\; \left(11^2\right)^2 \;\equiv\; (121)^2 \;\equiv\; 14641 \;\equiv\; 14641 - 22 \cdot 645 \;\equiv\; 451 \pmod{645}.$

$11^8 \;\equiv\; \left(11^4\right)^2 \;\equiv\; (451)^2 \;\equiv\; 203401 \;\equiv\; 203401 - 315 \cdot 645 \;\equiv\; 226 \pmod{645}.$

$11^{16} \;\equiv\; \left(11^8\right)^2 \;\equiv\; (226)^2 \;\equiv\; 51076 \;\equiv\; 51076 - 79 \cdot 645 \;\equiv\; 121 \pmod{645}.$

$11^{32} \;\equiv\; \left(11^{16}\right)^2 \;\equiv\; (121)^2 \;\equiv\; 451 \pmod{645}$ (from above).

$11^{64} \;\equiv\; \left(11^{32}\right)^2 \;\equiv\; (451)^2 \;\equiv\; 226 \pmod{645}.$

$11^{128} \;\equiv\; \left(11^{64}\right)^2 \;\equiv\; (226)^2 \;\equiv\; 121 \pmod{645}.$

$11^{256} \;\equiv\; \left(11^{128}\right)^2 \;\equiv\; (121)^2 \;\equiv\; 451 \pmod{645}.$

$11^{512} \;\equiv\; \left(11^{256}\right)^2 \;\equiv\; (451)^2 \;\equiv\; 226 \pmod{645}.$

Then, $11^{644} \;\equiv\; 11^{512+128+4} \;\equiv\; 11^{512} \cdot 11^{128} \cdot 11^4 \;\equiv\; 226 \cdot 121 \cdot 451 \pmod{645}$

$\equiv\; 12333046 \;\equiv\; 12333046 - 19121 \cdot 645 \;\equiv\; \boxed{1 \pmod{645}.}$

Note that Fermat's Little Theorem would have predicted this result *if* 645 was prime. As a result, we call 645 a *Fermat Pseudoprime.*

22. As before, we expand the exponent: $1001 = 512+489 = 512+256+233$

$= 512+256+128+105 = 512+256+128+64+41 = 512+256+128+64+32+9$

$= 512+256+128+64+32+8+1.$

Like before, we square, reduce modulo 101, and repeat, starting with 123:

$123^2 \equiv (123-101)^2 \equiv 22^2 \equiv 484 \equiv 484-4\cdot 101 \equiv 80 \pmod{101}.$

$123^4 \equiv \left(123^2\right)^2 \equiv 80^2 \equiv 6400 \equiv 6400-63\cdot 101 \equiv 37 \pmod{101}.$

$123^8 \equiv \left(123^4\right)^2 \equiv 37^2 \equiv 1369 \equiv 1369-13\cdot 101 \equiv 56 \pmod{101}.$

$123^{16} \equiv \left(123^8\right)^2 \equiv 56^2 \equiv 3136 \equiv 3136-31\cdot 101 \equiv 5 \pmod{101}.$

$123^{32} \equiv \left(123^{16}\right)^2 \equiv 5^2 \equiv 25 \pmod{101}.$

$123^{64} \equiv \left(123^{32}\right)^2 \equiv 25^2 \equiv 625 \equiv 625-6\cdot 101 \equiv 19 \pmod{101}.$

$123^{128} \equiv \left(123^{64}\right)^2 \equiv 19^2 \equiv 361 \equiv 361-3\cdot 101 \equiv 58 \pmod{101}.$

$123^{256} \equiv \left(123^{128}\right)^2 \equiv 58^2 \equiv 3364 \equiv 3364-33\cdot 101 \equiv 31 \pmod{101}.$

$123^{512} \equiv \left(123^{256}\right)^2 \equiv 31^2 \equiv 961 \equiv 961-9\cdot 101 \equiv 52 \pmod{101}.$

Then, $123^{1001} \equiv 123^{512+256+128+64+32+8+1} \pmod{101}$

$\equiv 123^{512}\cdot 123^{256}\cdot 123^{128}\cdot 123^{64}\cdot 123^{32}\cdot 123^{8}\cdot 123^{1} \pmod{101}$

$\equiv \left(123^{512}\cdot 123^{256}\right)\cdot\left(123^{128}\cdot 123^{64}\right)\cdot\left(123^{32}\cdot 123^{8}\right)\cdot\left(123^{1}\right) \pmod{101}$

$\equiv (52\cdot 31)\cdot(58\cdot 19)\cdot(25\cdot 56)\cdot(123) \equiv (1612)\cdot(1102)\cdot(1400)\cdot(123) \pmod{101}$

$\equiv (1612-15\cdot 101)\cdot(1102-10\cdot 101)\cdot(1400-13\cdot 101)\cdot(123-101) \pmod{101}$

(continued)

(continued) $\equiv (97)\cdot(92)\cdot(87)\cdot(22) \equiv (97\cdot 92)\cdot(87\cdot 22) \pmod{101}$

$\equiv (8924)\cdot(1914) \equiv (8924-88\cdot 101)\cdot(1914-18\cdot 101) \equiv (36)\cdot(96) \pmod{101}$

$\equiv 3456 \equiv 3456-34\cdot 101 \equiv \boxed{22 \equiv 123 \pmod{101}.}$

24. Assume that $|a| \leq |b|$. To find $\gcd(a, b)$, we let $r_0 = b$ and $r_1 = a$ and construct a sequence of integers (r_i's) using the division algorithm; specifically, for integers $i \geq 1$, we let

$$r_{i-1} = q_i \cdot r_i + r_{i+1}$$

where $q_i = \lfloor r_{i-1}/r_i \rfloor$ and $r_{i+1} = r_{i-1} - q_i \cdot r_i$.

Then, if $r_{k+1} = 0$ but $r_k \neq 0$ for some nonnegative integer k, then $\gcd(a, b) = r_k$.

(a) $\lfloor 5/1 \rfloor = \lfloor 5 \rfloor = 5$, and $5 - 5\cdot 1 = 0$, so we write $5 = 5\cdot 1 + 0$.

Then, $r_2 = 0$. Since $r_1 = 1 \neq 0$, we have $\gcd(1, 5) = \boxed{1.}$

(b) To begin, $101 = 1\cdot 100 + 1$.

Next, $100 = 100\cdot 1 + 0$.

Since the remainder in this integer division is zero, the remainder in the previous integer division is the greatest common divisor of the given pair of integers i.e. $\gcd(100, 101) = \boxed{1.}$

(c) $277 = 2\cdot 123 + 31$.

$123 = 3\cdot 31 + 30$.

$31 = 1\cdot 30 + 1$.

$30 = 30\cdot 1 + 0$.

So, $\gcd(123, 277) = \boxed{1.}$

(d) $14039 \ = \ 9 \cdot 1529 + 278.$

$1529 \ = \ 5 \cdot 278 + 139.$

$278 \ = \ 2 \cdot 139 + 0.$

Therefore, $\gcd(1529, 14039) \ = \ \boxed{139.}$

(e) $14038 \ = \ 9 \cdot 1529 + 277.$

$1529 \ = \ 5 \cdot 277 + 144.$

$277 \ = \ 1 \cdot 144 + 133.$

$144 \ = \ 1 \cdot 133 + 11.$

$133 \ = \ 12 \cdot 11 + 1.$

$11 \ = \ 11 \cdot 1 + 0.$

Accordingly, $\gcd(1529, 14038) \ = \ \boxed{1.}$

(f) $111111 \ = \ 10 \cdot 11111 + 1.$

$11111 \ = \ 11111 \cdot 1 + 0.$

Consequently, $\gcd(1529, 14038) \ = \ \boxed{1.}$

26. Let us perform the Euclidean algorithm and count the number of divisions that we did:

$$55 = 1 \cdot 34 + 21.$$

$$34 = 1 \cdot 21 + 13.$$

$$21 = 1 \cdot 13 + 8.$$

$$13 = 1 \cdot 8 + 5.$$

$$8 = 1 \cdot 5 + 3.$$

$$5 = 1 \cdot 3 + 2.$$

$$3 = 1 \cdot 2 + 1.$$

$$2 = 2 \cdot 1 + 0.$$

The number of divisions that the algorithm required was $\boxed{8.}$

The reason that it took so many was that 34 and 55 are consecutive *Fibonacci numbers.*