Training Problems #2 Solutions

Section 4.2:

26. In effect, this algorithm computes 11 **mod** 645, 11^2 **mod** 645, 11^4 **mod** 645, 11^8 **mod** 645, 11^{16} **mod** 645, ..., and then multiplies (modulo 645) the required values. Since $644 = (1010000100)_2$, we need to multiply

together 11^4 **mod** 645, 11^{128} **mod** 645, and 11^{512} **mod** 645, reducing modulo 645 at each step. We compute by repeatedly squaring: 11^2 **mod** $645 = 121$, 11^4 **mod** $645 = 121^2$ **mod** $645 = 14641$ **mod** $645 = 451$, 11^8 **mod** $645 = 451^2$ **mod** $645 = 203401$ **mod** $645 = 226$, 11^{16} **mod** $645 = 226^2$ **mod** $645 = 51076$ **mod** $645 = 121$. At this point we notice that 121 appeared earlier in our calculation, so we have 11^{32} **mod** $645 = 121^2$ **mod** $645 = 451$, 11^{64} **mod** $645 = 451^2$ **mod** $645 = 226$, 11^{128} **mod** $645 = 226^2$ **mod** $645 = 121$, 11^{256} **mod** $645 = 451$, and 11^{512} **mod** $645 = 226$. Thus our final answer will be the product of 451, 121, and 226, reduced modulo 645. We compute these one at a time: $451 \cdot 121$ **mod** $645 = 54571$ **mod** $645 = 391$, and $391 \cdot 226$ **mod** $645 = 88366$ **mod** $645 = 1$. So 11^{644} **mod** $645 = 1$. A computer algebra system will verify this; use the command “`1 &^ 644 mod 645;`” in *Maple*, for example. The ampersand here tells *Maple* to use modular exponentiation, rather than first computing the integer 11^{644}, which has over 600 digits, although it could certainly handle this if asked. The point is that modular exponentiation is much faster and avoids having to deal with such large numbers.

Section 4.3:

4. We obtain the answers by trial division. The factorizations are $39 = 3 \cdot 13$, $81 = 3^4$, $101 = 101$ (prime)

16. Since these numbers are small, the easiest approach is to find the prime factorization of each number and look for any common prime factors.

a) Since $21 = 3 \cdot 7$, $34 = 2 \cdot 17$, and $55 = 5 \cdot 11$, these are pairwise relatively prime.

b) Since $85 = 5 \cdot 17$, these are not pairwise relatively prime.

24. We form the greatest common divisors by finding the minimum exponent for each prime factor.

a) $2^2 \cdot 3^3 \cdot 5^2$ **b)** $2 \cdot 3 \cdot 11$ **c)** 17 **d)** 1

26. We form the least common multiples by finding the maximum exponent for each prime factor.

a) $2^5 \cdot 3^3 \cdot 5^5$ **b)** $2^{11} \cdot 3^9 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17^{14}$ **c)** 17^{17} **d)** $2^2 \cdot 5^3 \cdot 7 \cdot 13$

32. To apply the Euclidean algorithm, we divide the larger number by the smaller, replace the larger by the smaller and the smaller by the remainder of this division, and repeat this process until the remainder is 0. At that point, the smaller number is the greatest common divisor.

c) $\gcd(123, 277) = \gcd(123, 31) = \gcd(31, 30) = \gcd(30, 1) = \gcd(1, 0) = 1$