CSE 015: Discrete Mathematics
Homework #9 Solutions

Chapter 4.1

- 18(a): $12.11 = 143 \equiv 10 \pmod{19}$
- 18(f): $11^3 + 4.3^3 = 1439 \equiv 14 \pmod{19}$
- 22: Assume that $a \equiv b \pmod{m}$. This means that $m \mid a-b$, say $a-b = mc$, so that $a = b + mc$. Now let us compute a mod m. We know that $b = qm+r$ for some non-negative r less than m (namely, $r = b \bmod m$). Therefore we can write $a = qm + r + mc = (q + c)m + r$. By definition this means that r must also equal a mod m.
- 38(a): $(19^2 \bmod 41) \bmod 9 = (361 \bmod 41) \bmod 9 = 33 \bmod 9 = 6$
- 38(d): $(21^2 \bmod 15)^3 \bmod 22 = (441 \bmod 15)^3 \bmod 22 = 6^3 \bmod 22 = 216 \bmod 22 = 18$

Chapter 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: 451.121 mod 645 = 54571 mod 645 = 391, and 391.226 mod 645 = 88366 mod 645 = 1. So 11^{644} mod 645 = 1. A computer algebra system will verify this; use the command ”1 &ˆ 644 mod 645;” in Maple, for example. The ampersand here tells Maple to use modular exponentiation, rather than first computing the integer 11644, 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.

Chapter 4.3

- 4(e): 17^2
- 4(f): 29.31
- 16(c):Since $25 = 5^2$, 41 is prime, $49 = 7^2$, and $64 = 2^6$, these are pairwise relatively prime.
- 16(d):Since 17, 19, and 23 are prime and $18 = 2.3^2$, these are pairwise relatively prime.