HW 2.5 key

2. To convert from decimal to binary, we successively divide by 2. We write down the remainders so obtained from right to left; that is the binary representation of the given number.

a) Since 321/2 is 160 with a remainder of 1, the rightmost digit is 1. Then since 160/2 is 80 with a remainder of 0, the second digit from the right is 0. We continue in this manner, obtaining successive quotients of 40, 20, 10, 5, 2, 1, and 0, and remainders of 0, 0, 0, 0, 1, 0, and 1. Putting all these remainders in order from right to left we obtain $(1\ 0100\ 0001)_2$ as the binary representation. We could, as a check, expand this binary numeral: $2^0 + 2^6 + 2^8 = 1 + 64 + 256 = 321$.

b) We could carry out the same process as in part **(a)**. Alternatively, we might notice that $1023 = 1024 - 1 = 2^{10} - 1$. Therefore the binary representation is 1 less than $(100\ 0000\ 0000)_2$, which is clearly $(11\ 1111\ 1111)_2$.

c) If we carry out the divisions by 2, the quotients are 50316, 25158, 12579, 6289, 3144, 1572, 786, 393, 196, 98, 49, 24, 12, 6, 3, 1, and 0, with remainders of 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, and 1. Putting the remainders in order from right to left we have $(1\ 1000\ 1001\ 0001\ 1000)_2$.

20. In effect this algorithm computes powers $123 \bmod 101$, $123^2 \bmod 101$, $123^4 \bmod 101$, $123^8 \bmod 101$, $123^{16} \bmod 101$, ..., and then multiplies (modulo 101) the required values. Since $1001 = (1111101001)_2$, we need to multiply together $123 \bmod 101$, $123^8 \bmod 101$, $123^{32} \bmod 101$, $123^{64} \bmod 101$, $123^{128} \bmod 101$, $123^{256} \bmod 101$, and $123^{512} \bmod 101$, reducing modulo 101 at each step. We compute by repeatedly squaring: $123 \bmod 101 = 22$, $123^2 \bmod 101 = 22^2 \bmod 101 = 484 \bmod 101 = 80$, $123^4 \bmod 101 = 80^2 \bmod 101 = 6400 \bmod 101 = 37$, $123^8 \bmod 101 = 37^2 \bmod 101 = 1369 \bmod 101 = 56$, $123^{16} \bmod 101 = 56^2 \bmod 101 = 3136 \bmod 101 = 5$, $123^{32} \bmod 101 = 5^2 \bmod 101 = 25$, $123^{64} \bmod 101 = 25^2 \bmod 101 = 625 \bmod 101 = 19$, $123^{128} \bmod 101 = 19^2 \bmod 101 = 361 \bmod 101 = 58$, $123^{256} \bmod 101 = 58^2 \bmod 101 = 3364 \bmod 101 = 31$, and $123^{512} \bmod 101 = 31^2 \bmod 101 = 961 \bmod 101 = 52$. Thus our final answer will be the product of 22, 56, 25, 19, 58, 31, and 52. We compute these one at a time modulo 101: $22 \cdot 56$ is 20, $20 \cdot 25$ is 96, $96 \cdot 19$ is 6, $6 \cdot 58$ is 45, $45 \cdot 31$ is 82, and finally $82 \cdot 52$ is 22. So $123^{1001} \bmod 101 = 22$.

22. 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.

a) $\gcd(1,5) = \gcd(1,0) = 1$ **b)** $\gcd(100,101) = \gcd(100,1) = \gcd(1,0) = 1$

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

d) $\gcd(1529,14039) = \gcd(1529,278) = \gcd(278,139) = \gcd(139,0) = 139$

e) $\gcd(1529,14038) = \gcd(1529,277) = \gcd(277,144) = \gcd(144,133) = \gcd(133,11) = \gcd(11,1) = \gcd(1,0) = 1$

f) $\gcd(11111,111111) = \gcd(11111,1) = \gcd(1,0) = 1$