



(b)  $2^9 - 1 = 511$  is composite, by exercise 23. Specifically, it's equal to  $(2^3 - 1)(2^6 + 2^3 + 1) = 7 \cdot 73$ .

(c)  $2^{11} - 1 = 2047$  is equal to  $23 \cdot 89$ , so it's composite.

2.4 #32: Factor into primes:  $1000 = 2^3 5^3$  and  $625 = 5^4$ . Then  $\gcd(1000, 625) = 5^3 = 125$ , and  $\text{lcm}(1000, 625) = 2^3 5^4 = 5000$ . Check:  $125 \cdot 5000 = 625000 = 1000 \cdot 625$ .

2.4 #50: 3,6,4,3,6,4,...

2.4 Extra problem: to find  $p$  from  $q = f(p)$  we need to solve

$$q \equiv 3p + 7 \pmod{26}$$

for  $p$  in terms of  $q$ . Subtracting 7 gives

$$3p \equiv q - 7,$$

and multiplying by 9, using  $3 \cdot 9 \equiv 1$ , gives

$$p \equiv 9(q - 7) \equiv 9q + 15 \pmod{26}$$

The message BXP CHST VXU decrypts to YOU HAVE WON.