### Exercise 6.22

Show that if $p$ is prime, then $(p-2)! \equiv 1 \bmod (p)$. Show that if $p$ is an odd prime, then $(p-3)! \equiv (p-1)/2 \bmod (p)$.

### Exercise 6.23

Use Corollary 6.3 to show that there are infinitely many primes. (Take care to avoid a circular argument!)

### Exercise 6.24

For which Fermat primes and Mersenne primes is 2 a primitive root?

### Exercise 6.25

Find all the primitive roots for the integers $n = 18$ and 27. (Hint: see Exercises 6.4 and 6.5.)

### Exercise 6.26

(a) Show that if $p$ is an odd prime, and $g$ is a primitive root mod $(p)$ but not mod $(p^2)$, then $g + rp$ is a primitive root mod $(p^2)$ for $r = 1, 2, \ldots, p-1$. By counting primitive roots, deduce that if $g$ is a primitive root mod $(p)$ then exactly one of $g, g+p, g+2p, \ldots, g+(p-1)p$ is not a primitive root mod $(p^2)$.

(b) Find elements of $U_{25}$ congruent to $2, 3 \bmod (5)$ respectively, which are not primitive roots mod $(25)$.