Problem set 5

Problems 2 and 9(b) use results we will discuss on Monday.

1. So, Wilson’s theorem said that if \( m \) is prime, then \((m - 1)! \equiv -1 \mod m\).

   Check that the converse holds: i.e. that if \( m \) is composite then the congruence fails. (Of course, this is terribly inefficient as a primality test.)

2. Prove that if \( m \) is a Carmichael number, then it is of the form \( p_1 \cdots p_k \), where \( p_k \) are distinct primes with \( p_i - 1 | m - 1 \). You may use that \( m \) is odd. [Hint: a priori, \( m = \prod p_i^{r_i} \) for some odd primes \( p_i \). Use the Chinese remainder theorem together with a result on primitive roots.]

3. Apply the Miller-Rabin test to 2773. Is it composite or “likely prime”?

4. 8051 is composite. Factor it using Pollard’s \( \rho \) method.

5. Devise a test that will decide in polynomial time whether a given \( n \in \mathbb{N} \) is a perfect power, i.e., of the form \( a^b \) (where \( a, b \in \mathbb{N} \)). (You will recall that “polynomial” essentially means bounded by a constant times a power of \( \log(n) \).)

6. Let \( X \) be a large positive integer. Suppose that \( m \leq X/2 \), and that \( 0 \leq a < m \), \( 0 \leq b < m \). Explain why the number \( c \) determined by the following algorithm satisfies \( 0 \leq c < m \), and \( c \equiv (m)^{ab} \mod m \). Verify that in executing the algorithm, all numbers encountered lie in the interval \([0, X)\).

   1. Set \( k = b \), \( c = 0 \), \( g = \left\lfloor \frac{X}{m} \right\rfloor \).
   2. As long as \( a > 0 \), perform the following operations:
      (a) Set \( r = a - g \left\lfloor \frac{a}{g} \right\rfloor \).
      (b) Choose \( s \) so that \( s \equiv kr \mod m \) and \( 0 \leq s < m \).
      (c) Replace \( c \) by \( c + s \).
      (d) If \( c \geq m \), replace \( c \) by \( c - m \).
      (e) Replace \( k \) by \( gk - m \left\lfloor \frac{gk}{m} \right\rfloor \).
      (f) Replace \( a \) by \( \frac{a - r}{g} \).

7. Let \( d \) be a nonzero integer. Show that the ring \( \mathbb{Q}[\sqrt{d}] := \{ q_1 + q_2 \sqrt{d} | q_1, q_2 \in \mathbb{Q} \} \) is in fact a field.

8. Show that there are essentially (i.e. up to isomorphism) only two groups of order 4. [Hint: start by considering what are the possible orders of elements, keeping in mind only the identity “1” has order 1.]

9. (a) Which of the following groups are isomorphic: \( (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) \), \( (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \), \( \mathbb{Z}/24\mathbb{Z} \), \( S_4 \)?

   (b) What about \( \mathbb{Z}_{35}^* \)?