Solutions #3

1. 
   (a) Let \( k \) be a positive integer such that \( 2^k + 1 \) is a prime number. Prove that \( k = 2^t \) for some non-negative integer \( t \).

   (b) Let \( k > 1 \) be an integer such that \( 2^k - 1 \) is a prime number. Prove that \( k \) is prime itself.

Solution. (a) Assume, to the contrary, that \( k \) has an odd divisor \( m > 1 \). Let \( k = qm \).

Then

\[ 2^k + 1 = 2^{qm} + 1 = (2^q)^m + 1 = a^m + 1 = (a + 1)(a^{m-1} - a^{m-2} + \cdots + 1), \]

where \( a = 2^q \). The assumption \( m > 1 \) implies that \( 1 < a + 1 < a^m + 1 = 2^k + 1 \), and hence equation (1) shows that \( 2^k + 1 = a^m + 1 \) is not prime. This contradiction proves that \( k \) has no odd divisors other than 1, i.e., that \( k = 2^t \).

(b) Assume, to the contrary, that \( k \) is not prime, i.e., that \( k = uv \) with \( 1 < u, v < k \). Then

\[ 2^k - 1 = 2^{uv} - 1 = (2^u)^v - 1 = a^v - 1 = (a - 1)(a^{v-1} + a^{v-2} + \cdots + 1), \]

where \( a = 2^u \). The assumption \( u > 1 \) implies that \( 1 < a - 1 < a^v - 1 = 2^k - 1 \), and hence equation (2) shows that \( 2^k - 1 = a^v - 1 \) is not prime. This contradiction proves that \( k \) is prime.

Remark. The numbers of the form \( 2^{2^t} + 1 \) are known as Fermat numbers. Fermat conjectured that every such number is prime and verified that this is true for \( t = 0, 1, 2, 3, 4 \). Euler showed that 641 divides \( 2^{2^5} \) disproving Fermat’s conjecture. It is not known whether there are any Fermat primes other than the ones for \( 0 \leq t \leq 4 \).

The primes of the form \( 2^p - 1 \) are called Mersenne primes. So far 50 Mersenne primes are known, the latest was found in December 2017. Mersenne primes usually make the news with titles like “Mathematicians discovered the largest number”.

2. 
   (a) Prove that there are infinitely many primes of the form \( 4k + 3 \).

   (b) For every positive integer \( n \), show that there are (at least) \( n \) consecutive integers, none of which is prime.

Solution. (a) Assume that there are only finitely many positive primes of the form \( 4k + 3 \). Denote them by \( p_1, p_2, \ldots, p_N \). Consider \( P = 4p_1p_2 \ldots p_N + 3 \). \( P \) is an odd integer which is not a prime, since it is of the form \( 4k + 3 \) and is not on the list of all primes of this form (why?). Hence all prime divisors of \( P \) are of the form \( 4k + 1 \). But one checks immediately that the product of integers of the form \( 4k + 1 \) is still an integer of the same form, i.e. \( P \) is of the form \( 4k + 1 \). This contradiction shows that our
(b) Consider the integers 
\[(n + 1)! + 2, (n + 1)! + 3, \ldots, (n + 1)! + (n + 1).\]
For any \(2 \leq k \leq n + 1\), \(k\) divides \((n + 1)!\) (Why?) and hence \(k\) divides \((n + 1)! + k\). In particular, \((n + 1)! + k\) is not prime. Hence the numbers above provide an example of \(n\) consecutive numbers none of which is prime.

3. Let \(A = \{a, b, c\}\). Exhibit a relation on \(A\) with the stated properties.

(a) Reflexive, not symmetric, not transitive.
(b) Symmetric, not reflexive, not transitive.
(c) Transitive, not reflexive, not symmetric.
(d) Reflexive and symmetric, not transitive.
(e) Reflexive and transitive, not symmetric.
(f) Symmetric and transitive, not reflexive.

Solution. It is convenient to write relations as subsets \(R \subset A \times A\), where \((x, y) \in R\) exactly when \(x \sim y\). For example, the set \(\{(a, b), (b, c), (b, b)\} \subset A \times A\) means that we have the following relations (and only them) among \(a, b,\) and \(c\): \(a \sim b, b \sim c, b \sim b\).

(a) \(\{(a, a), (b, b), (c, c), (a, b), (b, c)\}\).
(b) \(\{(a, b), (b, a)\}\).
(c) \(\{(a, b)\}\).
(d) \(\{(a, a), (b, b), (c, c), (a, b), (b, a), (b, c), (c, b)\}\).
(e) \(\{(a, a), (b, b), (c, c), (a, b), (b, c), (c, a)\}\).
(f) \(\{(a, a), (b, b), (a, b), (b, a)\}\).

Remark. Most of these examples are not unique. For example, in (f) the empty set of relations also works.