Tutorial Sheet 6

Sept 6,8,9

1. Show that if a and b are both positive integers, then $(2^a - 1) \mod (2^b - 1) = 2^{a \mod b} - 1$.
2. Use the above to show that if a and b are positive integers, then $gcd(2^a - 1, 2^b - 1) = 2^{gcd(a,b)} - 1$. [Hint: Show that the remainders obtained when the Euclidean algorithm is used to compute $gcd(2^a - 1, 2^b - 1)$ are of the form $2^r - 1$, where r is a remainder arising when the Euclidean algorithm is used to find $gcd(a, b)$.]
3. Prove or disprove that $p_1 p_2 \cdots p_n + 1$ is prime for every positive integer n, where $p_1, p_2, ..., p_n$ are the n smallest prime numbers.
4. Use the Chinese remainder theorem to show that an integer a, with $0 \leq a < m = m_1 m_2 \cdots m_n$, where the positive integers $m_1, m_2, \ldots, m_n$ are pairwise relatively prime, can be represented uniquely by the n-tuple $(a \mod m_1, a \mod m_2, \ldots, a \mod m_n)$.
5. Show with the help of Fermat's little theorem that if n is a positive integer, then 42 divides $n^7 - n$.
6. Show that the system of congruences $x \equiv a_1 (\mod m_1)$ and $x \equiv a_2 (\mod m_2)$, where $a_1, a_2, m_1$and m_2 are integers with $m_1 > 0$ and $m_2 > 0$, has a solution if and only if $gcd(m_1, m_2)|(a_1 - a_2)$.
7. Show that if the system in the above question has a solution, then it is unique modulo $lcm(m_1, m_2)$.
8. Prove the correctness of the following rule to check if a number, N, is divsible by 7: Partition N into 3 digit numbers from the right $(d_3d_2d_1, d_6d_5d_4, \ldots)$. The alternating sum $(d_3d_2d_1 - d_6d_5d_4 + d_9d_8d_7 - \ldots)$ is divisible by 7 if and only if N is divisible by 7.
9. Show that if $ac \equiv bd (\mod m)$ then $a \equiv b (\mod (m/d))$ where $d = gcd(a, b)$.
10. How many zeroes are at the end of the binary expansion of $100_{10}!$?