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 $ac \equiv bc (\mod m)$ then $a \equiv b (\mod (m/d))$ where $d = gcd(c, m)$.
10. How many zeroes are at the end of the binary expansion of $100_{10}!$?

Solutions to Sheet 6

1. Let $a = bq + r, r = a \mod b$. Note $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \cdots + 1)$ and hence for all integer $k \geq 1, (x-1)|(x^k - 1)$. Choosing $x = 2^b$ we get $(2^b - 1)|(2^{bq} - 1)$ and hence $(2^a - 1) \mod (2^b - 1) = 2^r - 1 = 2^{a \mod b} - 1$.

2

We will prove this by induction. Let $P(a)$ be the stmt: $\forall 0 \leq b < a, \gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$. P(1) is true since for a=1, b=0, we get $\gcd(1, 0) = 2^{\gcd(1,0)} - 1 = 1$. We assume $P(i)$ is true, $1 \leq i \leq a$, and show that this implies $P(a+1)$. Now

$$\begin{aligned} \gcd(2^{a+1} - 1, 2^b - 1) &= \gcd(2^b - 1, (2^{a+1} - 1) \mod (2^b - 1))) \\ &= \gcd(2^b - 1, 2^{(a+1) \mod b} - 1) \\ &= 2^{\gcd(b,(a+1) \mod b)} - 1 \\ &= 2^{\gcd(a+1,b)} - 1 \end{aligned}$$

where the second equality follows from Q1, the third equality from $P(b)$ since $b \leq a$, and the first and fourth equalities from the fact that $\gcd(x, y) = \gcd(y, x \mod y)$.

3

Th eproduct of the first 6 prime numbers is 2.3.5.7.11.13 = 30030. The number $30031 = 59 \times 509$ and is composite thereby disproving the statement.

4

Suppose there exists distinct integers $a, b, 0 \leq a, b < m$, and the n-tuples corresponding to these integers are identical i.e $\forall i, 1 \leq i \leq n, a \equiv b(\mod m_i)$. Since the m_i are relatively prime, by Chinese remainder we get that $a \equiv b(\mod m)$ which implies that $m|(a - b)$. Since $0 \leq a, b < m$, $we\ get - m < (a - b) < m$. Hence $(a - b)$ is divisible by m iff $(a - b) = 0$ which is a contradiction since a and b are distinct.

5

By Fermat's little theorem, $7|(n^7 - n)$ and $3|(n^3 - n)$. From solution 1 it follows that $(n^2 - 1)|(n^6 - 1)$ and hence $(n^3 - n)|(n^7 - n)$. So $3|(n^7 - n)$. If n is odd then n^7 is odd and so $(n^7 - n)$ is even. If n is even then again $(n^7 - n)$ is even. Hence $2|(n^7 - n)$. Since 2,3,7 are co-prime we can apply Chinese remainder to conclude that $n^7 \equiv n(\mod 42)$.

6

The system of congruences has a solution iff $\exists k_1, k_2 \in \mathbb{Z}$, $k_1 m_1 + a_1 = k_2 m_2 + a_2$. Rearranging we get, $k_1 m_1 - k_2 m_2 = a_2 - a_1$. Note that $k_1 m_1 - k_2 m_2$ is an integer linear combination of m_1, m_2. Any integer linear combination of m_1, m_2 will be a multiple of $\gcd(m_1, m_2)$ and hence$\gcd(m_1, m_2)$ must divide $(a_2 - a_1)$.

Let $d = (a_2 - a_1)/\gcd(m_1, m_2)$. By the Extended Euclid's Algorithm we know that there exist s, t such that$s m_1 + t m_2 = \gcd(m_1, m_2)$. Hence, $k_1 = s \cdot d$ and $k_2 = -t \cdot d$ is a solution to $k_1 m_1 - k_2 m_2 = a_2 - a_1$and so $x = k_1 m_1 + a_1 = s d m_1 + a_1$is the solution to the system.

7

Suppose x, y are two solutions to the system of congruences. Then $x \equiv a_1(\mod m_1)$ and $y \equiv a_1(\mod m_1)$. Hence $x \equiv y(\mod m_1)$ and so $m_1|(x - y)$. Similarly $x \equiv y(\mod m_2)$ and so $m_2|(x - y)$. Thus $lcm(m_1, m_2)|(x - y)$ and hence $x \equiv y(\mod lcm(m_1, m_2))$.

8

Note that $1000 \equiv -1(\mod 7)$. By padding with zeros we can assume that n has 3k digits. and let n be $d_{3k} d_{3k-1} \ldots d_2 d_1$.Then $n = \sum_{i=1}^{k} d_{3i} d_{3i-1} d_{3i-2} 10^{3(i-1)}$ and so $n \equiv \sum_{i=1}^{k} (-1)^{i-1} d_{3i} d_{3i-1} d_{3i-2}(\mod 7)$. Thus n is divisible by 7 iff $(d_3 d_2 d_1 - d_6 d_5 d_4 + \cdots + (-1)^{k-1} d_{3k} d_{3k-1} d_{3k-2})$ is divisble by 7.

9

If $ac \equiv bc(\mod m)$ then $m|c(a - b)$ and so $(m/d)|(c/d)(a - b)$. Since $\gcd(m/d, c/d) = 1$, it should be the case that $(m/d)|(a - b)$. Hence $a \equiv b(\mod (m/d))$.

10

The number of zeroes in the binary expansion of a number n is the largest k such that 2^k divides n. Note that $\lfloor 100/2^i \rfloor$numbers between 1 and 100 are divisible by 2^i. Hence 100! is divisible by 2^k where $k = \lfloor 100/2 \rfloor + \lfloor 100/4 \rfloor + \lfloor 100/8 \rfloor + \lfloor 100/16 \rfloor + \lfloor 100/32 \rfloor + \lfloor 100/64 \rfloor = 50 + 25 + 12 + 6 + 3 + 1 = 97$.