Homework 1, solutions

Problem 1. Prove that every natural number is a sum of disctinct powers of 2 (e.g. $1 = 2^0$; $2 = 2^1$, $3 = 2^0 + 2^1$, etc.). Hint: Assume not and consider the smallest counterexample. Consider the case when it is even and the case when it is odd. Alternatively, prove it by induction.

Extra credit: prove that such expression is unique. Hint: Observe that $1 + 2 + 4 + \ldots + 2^n < 2^{n+1}$

Solution: We prove this by induction on n. The problem provides a verification of the result for $n = 1, 2, 3$. Suppose that $n \geq 1$ and the result is true for $1, 2, \ldots, n$. We want to justify that the result is true for $n + 1$. Note that $n + 1$ is either even or odd.

case 1: $n + 1 = 2k$ is even. Then $1 \leq k \leq n$, so we know that the result holds for k. In other words, $k = 2^{m_1} + 2^{m_2} + \ldots + 2^{m_s}$ for some integer $s \geq 1$ and integers $0 \leq m_1 < m_2 < \ldots < m_s$. But then

$$n + 1 = 2k = 2(2^{m_1} + 2^{m_2} + \ldots 2^{m_s}) = 2^{m_1+1} + 2^{m_2+1} + \ldots 2^{m_s+1}$$

is a sum of distinct powers of 2, so the result holds for $n + 1$.

case 2: $n + 1 = 2k + 1$ is even. Then again $1 \leq k \leq n$, so we know that the result holds for k, as in the first case. In other words, $k = 2^{m_1} + 2^{m_2} + \ldots + 2^{m_s}$ for some integer $s \geq 1$ and integers $0 \leq m_1 < m_2 < \ldots < m_s$. But then

$$n + 1 = 1 + 2k = 2^0 + 2(2^{m_1} + 2^{m_2} + \ldots + 2^{m_s}) = 2^0 + 2^{m_1+1} + 2^{m_2+1} + \ldots 2^{m_s+1}.$$

Since $0 < m_1 + 1 < m_2 + 1 < \ldots < m_s + 1$, $n + 1$ is a sum of distinct powers of 2, so the result holds for $n + 1$.

We proved the result for $n+1$ in both cases, hence, by the method of induction, the result is true for all integers $n \geq 1$.

Second proof. Here we give a different inductive proof. As before, suppose that $n \geq 1$ and the result is true for $1, 2, \ldots, n$. We want to justify that the result is true for $n+1$. There is an integer $k \geq 1$ such that $2^k \leq n+1 < 2^{k+1} = 2^k + 2^k$. If $n+1 = 2^k$, the result clearly holds for $n+1$. Otherwise, we have $0 < n+1-2^k < 2^k < n+1$.

It follows that the result holds for $n+1-2^k$, i.e. $n+1-2^k = 2^{m_1}+2^{m_2}+\ldots+2^{m_s}$ for some integer $s \geq 1$ and integers $0 \leq m_1 < m_2 < \ldots < m_s$. Clearly $m_s < k$ (since $n+1-2^k < 2^k$), so $n+1 = 2^{m_1}+2^{m_2}+\ldots+2^{m_s}+2^k$ and the result holds for $n+1$.

Suppose now that two different sums of distinct powers of 2 add to the same number. Thus, we have

$$2^{m_1}+2^{m_2}+\ldots+2^{m_s} = 2^{n_1}+2^{n_2}+\ldots+2^{n_t}$$

for some integers $s,t \geq 1$ and integers $0 \leq m_1 < m_2 < \ldots < m_s$, $0 \leq n_1 < n_2 < \ldots < n_t$. We may assume that $m_s \neq n_t$ (if $m_s = n_t$, we can cancel 2^{m_s} from both sides and still have two different sums of distinct powers of 2 adding to the same number). Without any loss of generality, we may assume that $m_s < n_t$. It follows that $2^{n_1}+2^{n_2}+\ldots+2^{n_t} \geq 2^{n_t}$ and

$$2^{m_1}+2^{m_2}+\ldots+2^{m_s} \leq 2^0+2^1+2^2+\ldots+2^{m_s} = 2^{m_s+1}-1 < 2^{m_s+1} \leq 2^{n_t}$$

which contradicts the equality $2^{m_1}+2^{m_2}+\ldots 2^{m_s} = 2^{n_1}+2^{n_2}+\ldots 2^{n_t}$.

Problem 2. We defined in class $v(n)$ to be the number of positive divisors of n. Charcterize positive integrs n such that $v(n) = 3$.

Solution: Since $v(n) = 3$, we must have $n > 1$ and n is not a prime. It follows that $n = pm$ for some prime number p and integer $m \geq 2$. Note that $1, p, m, pm$ are divisors of n, hence two of them must be equal. The only way this can happen is when $p = m$, so $n = p^2$ is a suqare of a prime. Conversly, if $n = p^2$ for some prime p then $1, p, p^2$ are the only divisors of n, so $v(n) = 3$.

Problem 3. Use the Euclidean algorithm to find the greatest common divisor d of 441 and 1155. Then find integers k, l such that $d = 441k + 1155l$. Verify your answer. **You should not use a calculator in this problem.**

Solution: Let us recall Euclid's algorithm. To find $\gcd(a,b)$ set $a_0 = b$, $a_1 = a$ and apply the following procedure: if $a_0, a_1, \ldots, a_n$ are already computed ($n \geq 1$) and $a_n = 0$ then stop: $a_{n-1} = \gcd(a,b)$. Otherwise, use division algorithm to get $a_{n-1} = k_n a_n + r_n$ with $0 \leq r_n < |a_n|$, set $a_{n+1} = r_n$, and repeat the procedure. It is easy to see that for any $m \geq 1$

$$\begin{pmatrix} a_m \\ a_{m+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -k_m \end{pmatrix} \begin{pmatrix} a_{m-1} \\ a_m \end{pmatrix}.$$

Thus

$$\begin{pmatrix} a_m \\ a_{m+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -k_m \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -k_{m-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -k_1 \end{pmatrix} \begin{pmatrix} b \\ a \end{pmatrix}.$$

We apply Euclid's algorithm with $a = 441 = a_1$ and $b = 1155 = a_0$: We have

$$a_0 = 1155 = 2 \cdot 441 + 273 = 2a_1 + 273;\ a_2 = 273$$

$$a_1 = 441 = 1 \cdot 273 + 168 = 1 \cdot a_2 + 168;\ a_3 = 168$$

$$a_2 = 273 = 1 \cdot 168 + 105 = 1 \cdot a_3 + 105;\ a_4 = 105$$

$$a_3 = 168 = 1 \cdot 105 + 63 = 1 \cdot a_4 + 63;\ a_5 = 63$$

$$a_4 = 105 = 1 \cdot 63 + 42 = 1 \cdot a_5 + 42;\ a_6 = 42$$

$$a_5 = 63 = 1 \cdot 42 + 21 = 1 \cdot a_6 + 21;\ a_7 = 21$$

$$a_6 = 42 = 2 \cdot 21 + 0 = 2 \cdot a_7 + 0;\ a_8 = 0$$

Thus $d = \gcd(1155, 441) = a_7 = 21$.

We can now work "backwards" to find

$$21 = 63-42 = 63-(105-63) = 2\cdot 63-105 = 2\cdot(168-105)-105 = 2\cdot 168-3\cdot 105 =$$

$$2\cdot 168-3\cdot(273-168) = -3\cdot 273+5\cdot 168 = -3\cdot 273+5\cdot(441-273) = 5\cdot 441-8\cdot 273 =$$

$$5 \cdot 441 - 8 \cdot (1155 - 2 \cdot 441) = -8 \cdot 1155 + 21 \cdot 441.$$

so $k = 21$, $l = -8$ work.

Alternatively, we can use the matrix interpretation of the algorithm, with $k_1 = 2, k_2 = 1, k_3 = 1, k_4 = 1, k_5 = 1, k_6 = 1, k_7 = 2$, which yields:

$$\begin{pmatrix} 21 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 1155 \\ 441 \end{pmatrix}.$$

Multiplying the matrices, we get

$$\begin{pmatrix} 21 \\ 0 \end{pmatrix} = \begin{pmatrix} -8 & 21 \\ 21 & -55 \end{pmatrix} \begin{pmatrix} 1155 \\ 441 \end{pmatrix}.$$

It follows that $21 = -8 \cdot 1155 + 21 \cdot 441$, so $l = -8$, $k = 21$ work.

Problem 4. Prove that if a, b are relatively prime integers such that $a|c$ and $b|c$ then $ab|c$. Hint: Write $ua + wb = 1$ for some integers u, w and use this to show that $b|c_1$, where $c = ac_1$.

Solution. We folow the hint. Since $a|c$ we have $c = ac_1$ for some integer c_1. Since a, b are relatively prime, there exist integers u, w such that $1 = ua + wb$. Multiplying the last equality by c_1, we arrive at $c_1 = uac_1 + wbc_1 = uc + bwc_1$. Since both uc and bwc_1 are clearly divisible by b, we conclude that $b|c_1$, i.e. $c_1 = bc_2$ for some integer c_2. It follows that $c = ac_1 = abc_2$, so $ab|c_2$.