# MATH 465 NUMBER THEORY, SPRING TERM 2025, SOLUTIONS 2

1. Prove that if $2^m+1$ is an odd prime, then there is an $n \in \mathbb{N}$ such that $m = 2^n$. These are the Fermat primes. Fermat thought that all numbers of the form $2^{2^n}+1$ are prime. Show that $641 | 2^{2^5}+1$.

$2^{16} = 65536 \equiv 154 \pmod{641}$, $2^{32} \equiv 154^2 = 23716 \equiv 640 \pmod{641}$

2. Let $n_1, n_2, \ldots, n_s \in \mathbb{Z}$, not all 0. Define $\mathrm{GCD}(n_1, n_2, \ldots, n_s)$ and prove that there exist integers $x_1, x_2, \ldots, x_s$ such that $n_1x_1 + n_2x_2 + \cdots + n_sx_s = \mathrm{GCD}(n_1, n_2, \ldots, n_s)$, and show that for every $j$ we have $(n_1, \ldots, n_s) | n_j$ and that if $d | n_j$ for every $j$, then $d | (n_1, \ldots n_j)$.

Define
$$\mathcal{D}(n_1, \ldots, n_s) = \{n_1x_1 + \cdots n_sx_s : x_j \in \mathbb{Z}\}.$$
Since there is an $n_j \neq 0$ we can choose $x_j = \pm 1$ and $x_i = 0$ for $i \neq j$, which shows that $\mathcal{D}(n_1, \ldots, n_s)$ has positive elements. Let $\mathrm{GCD}(n_1, \ldots, n_s)$ denote the least positive element.

For any $n_j$, by the division algorithm there are $q_j$ and $r_j$ so that $n_j = (n_1, \ldots, n_s)q_j + r_j$ and $0 \le r_j < (n_1, \ldots, n_s)$. $n_j$ and $(n_1, \ldots, n_s)$ are in $\mathcal{D}(n_1, \ldots, n_s)$. Hence so is $r_j$. But the minimality of $(n_1, \ldots, n_s)$ implies that $r_j = 0$ and so $(n_1, \ldots, n_s) | n_j$. On the other hand by definition there are $x_1, \ldots, x_s$ so that $(n_1, \ldots, n_s) = x_1n_1 + \cdots + x_sn_s$. Thus if $d | n_j$ for every $j$ then $d | x_1n_1 + \cdots + x_sn_s = (n_1, \ldots, n_s)$.

3. Let $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Prove that the equations $(x, y) = a$ and $xy = b$ can be solved simultaneously in integers $x$ and $y$ if and only if $a^2 | b$.

If $a^2 | b$, then take $x = a$, $y = b/a$. If $(x, y) = a$ and $xy = b$, then we have $x = au$, $y = av$ for some $u$, $v$ in $\mathbb{Z}$. Hence $a^2uv = xy = b$.

4. Find integers $x$ and $y$ such that $16801x + 2024y = (16801, 2024)$.

| | | | |
|---|---|---|---|
| | 16801 | 1 | 0 |
| 8 | 2024 | 0 | 1 |
| 3 | 609 | 1 | $-8$ |
| 3 | 197 | $-3$ | 25 |
| 10 | 18 | 10 | $-83$ |
| 1 | 17 | $-103$ | 855 |
| | 1 | 113 | $-938$ |

Thus $(16801, 2024) = (113)16801 - (938)2024 = 1$.