18.781, Fall 2007 Problem Set 1

Solutions of Selected Problems

Problem 1.2.2 We apply the Euclidean algorithm, as Example 1.

$$3587 = 1 \cdot 1819 + 1768$$

$$1819 = 1 \cdot 1768 + 51$$

$$1768 = 34 \cdot 51 + 34$$

$$51 = 1 \cdot 34 + 17$$

$$34 = 2 \cdot 17$$

This gives $(3587, 1819) = 17$.

Let's find x, y which satisfy $1819x + 3587y = 17$.

Starting with

$$1819 \cdot 0 + 3587 \cdot 1 = 3587.$$

and

$$1819 \cdot 1 + 3587 \cdot 0 = 1819.$$

We multiply the second of these equations by 1, and subtract the result from the first equation, to obtain

$$1819 \cdot (-1) + 3587 \cdot 1 = 1768.$$

We multiply this equation by 1, and subtract from the preceding equation to find that

$$1819 \cdot 2 + 3587 \cdot (-1) = 51.$$

We multiply this equation by 34, and subtract from the preceding equation to find that

$$1819 \cdot (-69) + 3587 \cdot 35 = 34.$$

We multiply this equation by 1, and subtract from the preceding equation to find that

$$1819 \cdot 71 + 3587 \cdot (-36) = 17.$$

Hence, we may take $x = 71, y = -36$. □

Problem 1.2.13 First, recall the fact that

$$\text{If } a_1 \mid c, \cdots, a_k \mid c \text{ and } (a_1, \cdots, a_k) = 1, \text{ then } a_1 \cdots a_k \mid c.$$

This can be proved directly from theorem 1.12.

1) $n^2 - n$
$n^2 - n = n(n-1)$. Since $n-1, n$ are consecutive integers, one of them is even. Hence, their product is clearly divisible by 2.

2) $n^3 - n$
$n^3 - n = (n-1)n(n+1)$. Since $n-1, n, n+1$ are three consecutive integers, one of them is a multiple of 3. This implies $3 \mid n^3 - n$. Also since $2 \mid n(n-1)$ and $n(n-1) \mid n^3 - n$, $2 \mid n^3 - n$. Because $(2,3) = 1$, the above fact tells that $6 \mid n^3 - n$, as desired.

3) $n^5 - n$
$n^5 - n = n(n^4 - 1) = (n-1)n(n+1)(n^2+1)$. Then $n^3 - n \mid n^5 - n$, so $n^5 - n$ is divisible by 6. Also, notice that every integer can be represented by $5k + r$ for proper $r = 0, \cdots, 4$. If $r = 0, 1, 4$, then $n, n-1, n+1$ is divisible by 5, respectively. If $r = 2, 3$, then $n^2 + 1 = (25k^2 + 20k + 5), (25k^2 + 30k + 10)$, respectively, and both are divisible by 5. Therefore, $5 \mid n^5 - n$. Since $(5,6) = 1$, This gives that $30 \mid n^5 - n$, as desired. □

Problem 1.2.36 Let $M = (a, b, c)$ and $N = ((a, b), c)$.
By definition, $M \mid a$ and $M \mid b$. This implies $M \mid (a, b)$ by theorem 1.4. Again by definition of M, $M \mid c$. Hence, $M \mid ((a, b), c) = N$, again by theorem 1.4.
Next, by definition of N, $N \mid (a, b)$ and $N \mid c$. Since $(a, b) \mid a$ and $(a, b) \mid b$, we can deduce that $N \mid a$ and $N \mid b$. Therefore N is a common divisor of a, b, c, so $N \mid (a, b, c) = M$.
Now we have got $M \mid N$and $N \mid M$. By theorem 1.1.(4), $M = \pm N$, but by definition, M, N are positive integers. Hence, $M = N$, as desired. □

Problem 1.2.46 First we prove the following fact.

For the integers x, y such that $(x, y) = 1$, $(x + y, x - y) = 1$ or 2.

Because $(x, y) = 1$, there is an integer s, t such that $sx + ty = 1$. Then

$$(s + t)(x + y) + (s - t)(x - y) = 2sx + 2ty = 2.$$

Hence $(x + y, x - y) \leq 2$ by theorem 1.4, so we just proved the above fact.

Now, suppose that there are positive integers a, b and $n > 1$ such that $(a^n - b^n) \mid (a^n + b^n)$. Note that we may assume $a > b$ without loss of generality. Then there is a positive integer Q which satisfies

$$(a^n + b^n) = Q(a^n - b^n).$$

Let $(a, b) = d$. Then divide this equation by d^n to find that

$$\left(\left(\frac{a}{d}\right)^n - \left(\frac{b}{d}\right)^n\right) = Q\left(\left(\frac{a}{d}\right)^n + \left(\frac{b}{d}\right)^n\right)$$

and $((\frac{a}{d}),(\frac{b}{d})) = 1$. Therefore, we can assume that there are positive integers a, b which are relatively prime with $a > b$, and $n > 1$ such that $(a^n - b^n) \mid (a^n + b^n)$.
$(a, b) = 1$ implies that $(a^n, b^n) = 1$, so we get

$$a^n - b^n = (a^n - b^n, a^n + b^n) = 1 \text{ or } 2,$$

where first equality holds by $(a^n - b^n) \mid (a^n + b^n)$ and second equality holds by the fact we proved first.
But $a^n - b^n = (a-b)(a^{n-1} + \cdots + b^{n-1})$ and it is trivial that $a \neq b$ to make $(a^n - b^n) \mid (a^n + b^n)$ a sense. So, $a > b \geq 1$. Therefore, $(a - b) \geq 1$ and $a^{n-1} + \cdots + b^{n-1} \geq 2 + 1 = 3$, since $n > 1$. Then we get

$$a^n - b^n = (a - b)(a^{n-1} + \cdots + b^{n-1}) \geq 3$$

a contradiction, because it cannot be 1 or 2. Therefore, there are no positive integers $a, b, n > 1$ such that $(a^n - b^n) \mid (a^n + b^n)$. □

Problem 1.2.50 By theorem 1.9,

$$(a + b, a^2 - ab + b^2) = (a + b, (a^2 - ab + b^2) - (a + b)(a + b)) = (a + b, -3ab) = (a + b, 3ab)$$

Let $d = (a + b, 3ab)$, and suppose that $(d, ab) \neq 1$. Then $(d, a) \neq 1$ or $(d, b) \neq 1$ by theorem 1.8. Without loss of generality, say $(d, a) \neq 1$. Let $e = (d, a) \geq 2$. Then $e \mid d$ and $e \mid a$. Also, $d \mid (a + b)$ implies that $e \mid (a + b)$, hence $e \mid b$. Then $(a, b) \geq e \geq 2$, a contradiction with the given condition $(a, b) = 1$. Therefore, $(d, ab) = 1$. Now, with the fact $d \mid 3ab$, we can have $d \mid 3$. So we can conclude that $d = 1$ or 3. □

Problem 1.3.5 First note that $(a + b) \mid (a^n + b^n)$ for odd n, and $(a - b) \mid (a^n - b^n)$ for any n. (I won't prove these facts here, but you can do this easily.)
Using this, for any integer m whose expression is $(a_k \cdots a_0) \quad (a_i \in \{0, \cdots 9\})$,

$$m = \sum_{i=0}^{k} a_i 10^i = \sum_{i \text{ is even}} a_i 10^i + \sum_{j \text{ is odd}} a_j 10^j$$

$$= \sum_{i \text{ is even}} a_i (10^i - 1) + \sum_{j \text{ is odd}} a_j (10^j + 1) + \sum_{i \text{ is even}} a_i - \sum_{j \text{ is odd}} a_j 10^j$$

Here, for even i, let $i = 2t$. Then, $99 \mid 100^t - 1 = 10^i - 1$, hence $11 \mid 10^i - 1$. For odd j, $11 = 10 + 1 \mid 10^j + 1$. Therefore, m is divisible by 11 if and only if $\sum_{i \text{ is even}} a_i - \sum_{j \text{ is odd}} a_j 10^j$ is divisible by 11. □

Problem 1.3.10 Suppose that there is an integer $m = 3k + 2$ which does not have a prime factor of the same form. Then

$$m = 3^s {p_1}^{e_1} \cdots {p_t}^{e_t}$$

where each p_i is the form $3k + 1$ and $s, e_i \geq 0$. Since $3 \nmid m$, we have $s = 0$. Any product of two integers who have the form $3k + 1$ also have the form $3k + 1$, so we conclude that m is of the form $3k + 1$, which is a contradiction.

Thus, there is no such m, so any positive integer of the form $3k+2$ has a prime factor of the same form.
The cases of $4k+3$ and $6k+5$ can be proved similarly. □

Problem 1.3.26 Suppose there are only finitely many primes of the form $4n+3$. Let $p_1, \cdots, p_k$ are all the such primes, with $p_1 = 3$. Note that $k \geq 2$ clearly. Consider a number $M = 4p_2 \cdots p_k + 3$. Then M is of the form $4n+3$, hence M has the prime factor p of the form $4n+3$ by exercise 1.3.10. By assumption, p should be the one of the p_i's. But it is easy to observe that any p_i cannot divide M, so it is a contradiction. Thus, there are infinitely many primes of the form $4n+3$.
The case of $6n+5$ can be proved similarly. □

Problem 1.3.31 We can easily verify the following fact using $(a-b) \mid (a^n - b^n)$ for any n .

For any polynomial $f(x)$ with integral coefficients, $m-n \mid f(m)-f(n)$ holds for any integers m, n.

Now suppose that there is a polynomial $f(x)$ of degree > 1 with integral coefficients can represent a prime for every positive integer x. And let $f(1) = p$. By the above fact, $p \mid f(pk+1) - f(1)$ for any nonnegative integer k. That is, $p \mid f(pk+1)$.
Let $g(x) = f(px+1) - f(1)$. Then $g(x)$ is a polynomial of same degree with $f(x)$. Hence $g(x) = 0$ have only finitely many roots. It implies that there is a nonnegative integer s such that $f(ps+1) \neq f(1) = p$. Then, $f(ps+1)$ is divisible by prime p , but it is not p. This implies that $f(ps+1)$ $(ps+1 \geq 1)$ is not a prime number, which is a contradiction. Therefore, there is no such polynomial. □
REMARK) I think that we may assume degree of $f(x) \geq 1$ instead of > 1.

Problem 1.3.48 First we prove the following fact.

For different positive integers n, m, $\left(2^{2^n}+1, 2^{2^m}+1\right) = 1$.

Without loss of generality, let $n < m$. Then $\left(2^{2^n}+1\right)\left(2^{2^n}-1\right) = \left(2^{2^{n+1}}-1\right)$. Using this repeatedly, we can conclude that $2^{2^n}+1 \mid 2^{2^m}-1$. Thus,

$$\left(2^{2^n}+1, 2^{2^m}+1\right) = \left(2^{2^n}+1, 2^{2^m}-1+2\right) = \left(2^{2^n}+1, 2\right) = 1,$$

where the last equality holds because $2^{2^n}+1$ is clearly odd.

We just prove that any two elements of the given sequence are relatively prime.
Using this fact, we now prove that there are infinitely many primes.
Since each $2^{2^n}+1$ is bigger than 1, there is at least one prime which is a prime divisor of $2^{2^n}+1$. That chosen prime numbers are all distinct because any two elements of sequence

are relatively prime. Since this sequence have infinitely may different terms, we can conclude that there are infinitely many prime numbers. □

If you have any question, please contact me : Yoonsuk Hyun (yshyun@math.mit.edu)