MATH6222: Homework #6

2017-04-04

Instructor: Dr. David Smyth

Tutor: Mark Bugden (Wednesday 1-2pm)

Rui Qiu u6139152

Problem 1

Let $a, b \in \mathbb{Z}$,
(a) Prove that $\gcd(a+b, a-b) = gcd(2a, a-b) = gcd(a+b, 2b)$.
(b) Suppose that $\gcd(a, b) = 1$. What can you say about $\gcd(a^2, b^2)$? What about $\gcd(a, 2b)$?

(a) Proof: Suppose $d \in \mathbb{Z}, d|(a+b), d|(a-b)$, then we claim that d divides the sum and difference of such two integers:

$$\begin{aligned} d|(a+b+a-b) &\implies d|(2a) \\ d|(a+b-a+b) &\implies d|(2b) \end{aligned}$$

The reasoning is, suppose $\exists\ k, j \in \mathbb{Z}, a+b = dk, a-b = dj$, then

$$\begin{aligned} 2a = a+b+a-b = d(k+j) \\ 2b = a+b-a+b = d(k-j) \end{aligned}$$

For the same reasoning, when we have $d|(2a), d|(a-b)$, then automatically we have

$$\begin{aligned} d|(2a-a+b) &\implies d|(a+b) \\ d|(a+b-a+b) &\implies d|(2b) \end{aligned}$$

Similarly, when we have $d|(a+b), d|(2b)$, we have the following at the same time:

$$\begin{aligned} d|(a+b-2b) &\implies d|(a-b) \\ d|(a+b+a-b) &\implies d|(2a) \end{aligned}$$

To conclude, for the 3 pairs of integers, if we have a common divisor d for one of the pairs, then it is automatically a common divisor of the other two pairs. This is equivalent to say, the set of common divisors of the 3 pairs are the same. So the **greatest** common divisors of the 3 pairs are the same.

$\blacksquare$

(b) Proof: Suppose $a = p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}, b = q_1^{l_1} q_2^{l_2} \cdots q_j^{l_j}$, where all p's and q's are prime factors (reordered with $p_1 < p_2 < \cdots < p_i$ and $q_1 < q_2 < \cdots < q_j$ for simplicity), and k's and l's are integers.

Since $\gcd(a, b) = 1$, $p_s \neq q_t$ for any integers $1 < s < i, 1 < t < j$.

Simply squaring a, b will only double the exponents of prime factorizations of a and b, i.e.

Problem 1 continued on next page. . .

$$a^2 = p_1^{2k_1} p_2^{2k_2} \cdots p_i^{2k_i}$$
$$b^2 = q_1^{2l_1} q_2^{2l_2} \cdots q_j^{2l_j}$$

Still, $p_s \neq q_t$ for any prime factors of a and b, no more common factors added. The greatest common divisor of a and b remains the same, i.e. $\gcd(a^2, b^2) = \gcd(a, b) = 1$.

However, when it comes to $\gcd(a, 2b)$, there are two possible cases:

- If a has no prime factor 2, then $2b = 2q_1^{l_1} q_2^{l_2} \cdots q_j^{l_j}$ has an extra prime factor 2 which is still a "common" factor, so the greatest common divisor won't change.
- If a has prime factor 2 already as $a = 2p_2^{k_2} \cdots p_i^{k_i}$, then $2b$ will give our pair a new common factor 2, i.e. $\gcd(a, 2b) = 2 \neq \gcd(a, b) = 1$.

To conclude, $\gcd(a^2, b^2) = 1$ but $\gcd(a, 2b) = 1$ or 2.

■

Problem 3

Show that the gaps between primes can be arbitrarily large. Do this by constructing, for any positive integer n, a set of n consecutive integers that are not prime. (Hint: Determine a positive integer x such that x is divisible by $2, x+1$ is divisible by $3, x+2$ is divisible by 4, etc.)

Proof: Suppose such set S contains consecutive non-prime integers starting from x with cardinality n.

$$S = \{x, x+1, x+2, \ldots, x+n-1\}$$

Also according to the hint, we would like to have $2|x, 3|(x+1), 4|(x+2), \ldots, (n+1)|(x+n-1)$.

Since $(n+1)! = 1 \cdot 2 \cdots (n+1)$, $(n+1)!$ is divisible by n consecutive integers from 2 to $n+1$. If x equals to $(n+1)!$, we obviously have $2|x$, but we are not sure about $3|((n+1)!+1)$.

How are we gonna fix this? We know that $(n+1)! + 3 = 3(2 \cdot 4 \cdot 5 \cdot 6 \cdots (n+1) + 1)$. And similarly, $(n+1)! + 4 = 4(2 \cdot 3 \cdot 5 \cdot 6 \cdots (n+1) + 1)$.

Therefore, we define $x = (n+1)! + 2$ instead of just $(n+1)!$, then we will have n consecutive non-prime integers, namely, $x, x+1, \ldots, x+n-1$, which are divisible by $2, 3, 4, \ldots, n-1$ correspondingly.

Problem 3 continued on next page. . .

Hence, for integer n, if we make n arbitrarily large, then there are always n number of consecutive integers that are not prime, i.e. the gap between primes is arbitrarily large.

■

Problem 4

Let p be a prime number.
(a) Prove that p divides $\binom{p}{k}$ for any $1 \leq k \leq p-1$.
(b) Prove that $n^p - n$ is divisible by p for every $n \in \mathbb{N}$. (Hint: Use the binomial theorem and part (a) in a proof by induction.)

(a) Proof: We can expand $\binom{p}{k}$:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{(p-k+1)\cdot(p-k+2)\cdots p}{1\cdot 2\cdot 3\cdots k}$$

Since p is a prime number, which is only divisible by 1 and itself, it cannot be canceled out by any integers in the interval $1 \leq k \leq p-1 < p$ in the denominator. So $\binom{p}{k} = p \cdot K$, where $K = \frac{(p-k+1)\cdot(p-k+2)\cdots(p-1)}{1\cdot 2\cdot 3\cdots k}$, i.e. $p|\binom{p}{k}$.

■

(b) Proof: Proof by induction on n.

Base step: $n = 1, n^p - n = 1^p - 1 = 0$ for prime p. And by convention, 0 is divisible by p.

Inductive hypothesis: Suppose $n = k$, we claim that $k^p - k$ is divisible by prime p.

We want to show for $n = k+1$, $(k+1)^p - (k+1)$ is divisible by prime p as well.
Recall the Binomial Theorem which states that:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

Specifically,

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i.$$

where a, b are integers. And we apply it on our desired formula:

Problem 4 continued on next page...

$$
\begin{aligned}
(k+1)^p - (k+1) &= \sum_{i=0}^{p} \binom{p}{i} k^i \cdot 1^{p-i} - (k+1) \\
&= \sum_{i=0}^{p} \binom{p}{i} k^i - (k+1) \\
&= \sum_{i=0}^{p-1} \binom{p}{i} k^i + \binom{p}{p} k^p - k - 1 \\
&= \binom{p}{0} k^0 + \sum_{i=1}^{p-1} \binom{p}{i} k^i + (k^p - k) - 1 \\
&= \sum_{i=1}^{p-1} \binom{p}{i} k^i + (k^p - k)
\end{aligned}
$$

By part (a), $\binom{p}{i}$ is divisible by p for any $1 \leq i \leq p-1$, so the sum of $\binom{p}{i}$ is also divisible by p.

By inductive hypothesis, $k^p - k$ is divisible by p.

Therefore, as the sum of sum of combinations $\binom{p}{i}$ and $k^p - k$, $(k+1)^p - (k+1)$ is also divisible by p, i.e. we've proved the case for $n = k+1$.

Hence $n^p - n$ is divisible by p for every $n \in \mathbb{N}$.

∎