Homework 1

Wenqi He

December 2, 2018

1

1.1

All p_i's are odd, so their product must be odd. Therefore $p_1 p_2 \cdots p_n$ has either the form $4k+3$ or $4k+1$. Note that

$$(4k+3)^2 = 16k^2 + 24k + 9 = 4(4k^2 + 6k + 2) + 1$$
$$(4k+1)^2 = 16k^2 + 8k + 1 = 4(4k^2 + 2k) = 1$$

which means that $(p_1 p_2 \cdots p_n)^2$ is of the form $4k+1$. Adding 2 gives the form $4k+3$.

1.2

Suppose there exists a p_i that divides M. Since $p_i | (p_1 p_2 \cdots p_n)^2$,

$$p_1 \Big| \Big(M - (p_1 p_2 \cdots p_n)^2 \Big)$$

or equivalently $p_1 | 2$. However, $p_i \geq 3$ by definition, so it cannot divide 2. This is a contradiction, which means that no p_i can divide M.

1.3

If M is prime, then it already contradicts the hypothesis that p_i's are all the primes of the form $4k+3$, since M would be a new prime of that form and it's larger than any of the p_i's. Now suppose M is composite. Note that: *i*) Since M is odd, it cannot be divided by 2. *ii*) From the result of 1.2, none of p_i's divide M, and since we assumed that p_i's are the only primes of the form $4k+3$, no prime of the form $4k+3$ divides M. Thus we conclude that $M = \prod q_i$ where q_i's have the form $4k+1$. However, that cannot be true, because if we have $a = 4m+1$ and $b = 4n+1$, then

$$ab = (4m+1)(4n+1) = 16mn + 4m + 4n + 1 = 4(4mn + m + n) + 1$$

It can be shown inductively that $M = \prod q_i$ must be of the form $4k+1$, which is a contradiction because we already showed that M is of the form $4k+3$.

2

Suppose there are only a finite number of primes of the form $3k+2$, Let $p_1 = 2, p_2 = 5, \cdots, p_n$ denote the n primes. Consider

$$M = 3 \prod_{i=2}^{n} p_i + 2$$

M is of the form $3k+2$, so if it is prime then we already have an contradiction, because it would be a prime of the form $3k+2$ that's not included in $\{p_i\}$. Now suppose it's composite. Obviously it's not divisible by 3 because $3 \nmid 2$. M is also not divisible by p_i, because we know that

$$p_i \mid 3\prod_{i=2}^{n} p_i$$

If $p_i \mid M$ then $p_i \mid 2$, which cannot be true because the only prime that divides 2 is 2, and we excluded $p_1 = 2$ when constructing M. Since 3 is the only prime of the form $3k$, and we assumed that p_i's are the only primes of the form $3k+2$, it must be true that M is a product of primes of the form $3k+1$ only. However, that cannot be true because the product of any two number of the form $3k+1$ is still $3k+1$:

$$(3m+1)(3n+1) = 3(3mn+m+n)+1$$

Therefore the hypothesis that there are only finitely many primes of the form $3k+2$ is false, meaning there are infinitely many such primes.

3

3.1

$$\begin{aligned} 561 &= 22 \cdot 25 + 11 \\ 25 &= 2 \cdot 11 + 3 \\ 11 &= 3 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

$gcd(561, 25) = gcd(25, 11) = gcd(11, 3) = gcd(3, 2) = gcd(2, 1) = 1$

3.2

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (11 - 3 \cdot 3) \\ &= -1 \cdot 11 + 4 \cdot 3 \\ &= -1 \cdot 11 + 4 \cdot (25 - 2 \cdot 11) \\ &= 4 \cdot 25 - 9 \cdot 11 \\ &= 4 \cdot 25 - 9 \cdot (561 - 22 \cdot 25) \\ &= -9 \cdot 561 + 202 \cdot 25 \end{aligned}$$

$x = -9$ and $y = 202$

1.1.16

$$\{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\}$$

1.1.22

$$\{i^2 + 2 : i \in \mathbb{Z}^+\}$$

1.1.28

$$\{\frac{3i}{4} : i \in \mathbb{Z}\}$$