MTH 505 Homework 3

Roy Howie

March 6, 2017

3.1 Infinitely Many Primes

Suppose there is a finite number of positive primes $p_1, p_2, \cdots, p_k$ and consider the number $N = 1 + \prod_{i=1}^{k} p_i$. Note that $N \geq 2$, so it must have a positive prime factor q. Furthermore, for all i, one has $N \equiv 1 \pmod{p_i}$. But q divides N, so there is no p_i equal to q. This is a contradiction, as we assumed our list contained all positive prime numbers. Hence, no such finite list exists. $\square$

3.2 Infinitely Many Primes $\equiv$ 3 Modulo 4

Let $n \equiv 3 \pmod 4$ be a positive integer, then it can be written as the product of positive primes: $p_1 p_2 \cdots p_k$. Note that p_i is either equal to 1 or 3 modulo 4. Assume $p_i \equiv 1 \pmod 4$ for all i. This is a contradiction, as then $n \equiv p_1 p_2 \cdots p_k \equiv 1 * 1 * \cdots * 1 \equiv 1 \pmod 4$. But we assumed $n \equiv 3 \pmod 4$. Hence, n has at least one prime factor which is 3 modulo 4.

Next, suppose there is a finite number of primes congruent to 3 modulo 4: $3 < p_1 < p_2 < \cdots < p_k$. Consider $N = 3 + 4\prod_{i=1}^{k} p_i$. Note that $N \equiv 3 \pmod 4$, so it has a prime factor $q \equiv 3 \pmod 4$. Furthermore, note that, for all i, one has $N \equiv 3 \pmod{p_i}$. But q divides N, so there is no p_i equal to q. This is a contradiction, as our list purportedly contained all primes congruent to 3 modulo 4. Therefore, no such finite list exists. $\square$

3.3 Infinitely Many Primes $\equiv$ 1 Modulo 4

Suppose there is a finite number of primes congruent to 1 modulo 4: $p_1, p_2, \cdots, p_k$. Let $x = 2p_1 p_2 \cdots p_k$ and consider $N = 1 + x^2$. Note that $N \equiv 1 \pmod 4$, as $4 \mid x^2$. Furthermore, for all i, one has $p_i \mid x$, so $N \equiv 1 \pmod{p_i}$.

If N is prime, this is a contradiction, for then there is a prime number congruent to 1 modulo 4 not found in the above list.

Otherwise, N has a prime divisor q. Let φ be the totient function and note that $\varphi(q) = q - 1$. But then $x^2 \equiv N - 1 \equiv -1 \pmod q$, so $x^4 \equiv 1 \pmod q$. This implies $4 \mid (q-1)$, or that $q \equiv 1 \pmod 4$. Recall that none of the primes in our list divided N. However, $q \mid N$, so q is a prime congruent to 1 modulo 4 not present in our list of primes. This is a contradiction, as our list supposedly contained all primes congruent to 1 modulo 4.

Hence, no such list exists. $\square$

3.4 A Useful Lemma

Let $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$. We wish to show $a \mid c$ and $b \mid c$ implies $ab \mid c$.

Note that there exist $d, e, x, y \in \mathbb{Z}$ such that $ad = c = be$ and $ax + by = 1$. Thus,

$$c = cax + cby = (be)ax + (ad)by = ab(ex + dy)$$

So ab divides c. $\square$

3.5 Generalization of Euler's Totient Theorem

Let n be a positive integer with prime factorization $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Let $e, f \in \mathbb{Z}$ such that $e_i \leq e$ and $\varphi(p_i^{e_i}) \mid f$ for all i. Fix $a \in \mathbb{Z}$.

For each p_i, either p_i divides a or p_i does not divide a. If p_i divides a, note that $p_i^{e_i}$ divides a^e, as $e_i \leq e$.

Conversely, if p_i does not divide a, then a and $q = p_i^{e_i}$ are coprime. Let $d = \varphi(q)$. Then, by Euler's Totient Theorem, one has $a^d \equiv 1 \pmod{q}$. But $\varphi(q)$ divides f, so $a^f \equiv 1 \pmod{q}$. Equivalently, $q = p_i^{e_i}$ divides $a^f - 1$.

Therefore, $p_i^{e_i}$ divides $a^e(a^f - 1)$ for every p_i. Hence, by **(3.4)**, one must have that $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = n$ divides $a^e(a^f - 1)$.

Thus, $a^{f+e} \equiv a^e \pmod{n}$. $\square$

3.6 RSA Cryptosystem

Let $p, q \in \mathbb{Z}$ be prime. Let $n = pq$, $e = 1$, and $f = \varphi(pq) = (p-1)(q-1)$.

Then, for all $a \in \mathbb{Z}$, one has via **(3.5)** that $a^{f+e} \equiv a^e \pmod{pq}$. This is equivalent to $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$. $\square$