

Math 110A Homework #2

David Wihr Taylor

Summer 2006

1. Problem 1.3.1: Express each number as the product of primes: (a) 5040, (b) -2345 , (c) 45670, (d) 2042040.

Answer: To my knowledge there is no fast algorithm to factor primes that doesn't use quantum computing (see Shore's algorithm if you want to see how to factor on a quantum computer). If there were some conventional algorithm, then all computer encryption would be unsafe (same thing if anyone ever builds a quantum computer)! However, there is an algorithm that runs as a polynomial function of the size of the number you input that tells you *if* your number is prime. All this basically doesn't help you do this problem, but it's interesting stuff anyway.

Mathematica tells me:

- (a) $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$
(b) $-2345 = -1 \cdot 5 \cdot 7 \cdot 67$
(c) $45670 = 2 \cdot 5 \cdot 4567$
(d) $2042040 = 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17$.

2. Problem 1.3.9:

Claim. *If p is prime and $(a, b) = p$ then $(a^2, b^2) = p^2$*

Proof. First we notice that if p divides both a and b then p^2 divides both a^2 and b^2 . Now let's express a and b by their prime factorizations $a = p_1^{r_1} \cdots p_k^{r_k}$ and $b = q_1^{s_1} \cdots q_l^{s_l}$. Then since $(a, b) = p$ we know that for one and only one pair (i, j) does $p_i = q_j = p$ and furthermore $r_i = s_j = 1$. That is, the only common factor of a and b is p , otherwise we could just multiply some other common factor by p to get a bigger common factor! Then since $a^2 = p_1^{2r_1} \cdots p_k^{2r_k}$ and $b^2 = q_1^{2s_1} \cdots q_l^{2s_l}$, (a^2, b^2) is only divisible by common factors of a and b . The only common factor of a and b is p . Thus if $c = (a^2, b^2)$ then $p|c$. Now from the above prime factorizations we see that the biggest power of p that divides both a^2 and b^2 is p^2 . Thus $p^2 = (a^2, b^2)$. □

3. Problem 1.3.20:

- (a) Prove that there are no integers a and b such that $a^2 = 2b^2$.
(b) Prove that $\sqrt{2}$ is irrational

Proof. (a) Let $a = p_1^{r_1} \cdots p_k^{r_k}$ and $b = q_1^{s_1} \cdots q_l^{s_l}$ be prime factorizations of a and b . Then $a^2 = p_1^{2r_1} \cdots p_k^{2r_k}$ and $b^2 = q_1^{2s_1} \cdots q_l^{2s_l}$ are prime factorizations of a^2 and b^2 . Then for some i , $p_i^{2r_i} = 2$. This implies that $p_i = 2$ and $2r_i = 1$. This is a contradiction since r_i must be an integer!

(b) If $\sqrt{2}$ is rational then $\sqrt{2} = a/b$ for some integers a and b . Then $2 = a^2/b^2$ which implies that $a^2 = 2b^2$. By part (a) we know this cannot happen. Therefore $\sqrt{2}$ is irrational. □

4. Problem 1.3.23:

(Euclid) Prove that there are infinitely many primes.

Proof. We proceed by contradiction:

Assume that there are finitely many primes which we list: p_1, \dots, p_k . Then consider the product $n = p_1 \cdots p_k + 1$. Then n has remainder 1 when divided by each prime, and so must either be prime itself or a product of primes not on our list. This is a contradiction since we assumed our list had all the primes. □

5. Problem 2.1.1: If $a \equiv b \pmod{n}$ and $k \mid n$, is it true that $a \equiv b \pmod{k}$?

Yes! $a \equiv b \pmod{n}$ implies that $a = b + l \cdot n$. Then $k \mid n$ implies that $n = q \cdot k$. Therefore $a = b + l \cdot q \cdot k$, and we obtain the equality, $a \equiv b \pmod{k}$.

6. Problem 2.1.9: Prove that

(a) $(n - a)^2 \equiv a^2 \pmod{n}$

(b) $(2n - a)^2 \equiv a^2 \pmod{4n}$

Proof. (a) $(n - a)^2 = n^2 - 2an + a^2$. Therefore, the remainder mod n is a^2 .

(b) $(2n - a)^2 = 4n^2 - 4an + a^2$. Therefore, the remainder mod $4n$ is a^2 . □

7. Problem 2.1.16:

(a) If a is a nonnegative integer, prove that a is congruent to its last digit mod 10.

(b) Show that no perfect square has 2,3,7, or 8 as its last digit.

Proof. (a) Let a have the base-ten representation $a = \sum_{i=0}^n a_i \cdot 10^i$ where $a_i \in \mathbb{Z}$ and $0 \leq a_i \leq 9$. Then $a \equiv a_0 \pmod{10}$. This is what we wanted to show.

(b) $a^2 = (\sum_{i=0}^n a_i \cdot 10^i)^2 = (\sum_{i=1}^n a_i \cdot 10^i + a_0)^2 = (\sum_{i=1}^n a_i \cdot 10^i)^2 + 2(\sum_{i=1}^n a_i \cdot 10^i)a_0 + a_0^2$. Then $a^2 \equiv a_0^2 \pmod{10}$. So we only need classify the remainders of a_0^2 modulo 10 to finish. $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16$, $5^2 = 25$, $6^2 = 36$, $7^2 = 49$, $8^2 = 64$, $9^2 = 81$ so the only possible remainders are 0, 1, 4, 5, 6 and 9. Then a perfect square can't have last digit 2, 3, 7, or 8. □

8. Problem 2.1.17:

Prove that $a \equiv b \pmod{n}$ if and only if a and b have the same remainder mod n .

Proof. First let's use division with remainder to write $a = q_1n + r_1$ and $b = q_2n + r_2$. If $a \equiv b \pmod{n}$ then we know that $(a - b) = (q_1 - q_2)n + (r_1 - r_2) = l \cdot n$. Then we have that $r_1 - r_2 = (l + q_2 - q_1)n$. Then we know $r_1 \equiv r_2 \pmod{n}$. But since $0 \leq r_1, r_2 < n$, we must have $r_1 - r_2 = 0$. Thus $r_1 = r_2$.

Conversely, assume $a = q_1 \cdot n + r$ and $b = q_2 \cdot n + r$, that is they have the same remainder when divided by n . Then $a - b = (q_1 - q_2)n$, which means that $a \equiv b \pmod{n}$. □