Math 300.2 Homework 7

Paul Hacking

October 31, 2017

Reading: Sundstrom, Sections 8.2 and 8.3.

Recall the fundamental theorem of arithmetic: Every positive integer n can be written as a product of primes in a unique way (up to reordering the factors). So, collecting equal prime factors together, we can write

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

where $r \in \mathbb{Z}_{\geqslant 0}$, $p_1, p_2, \ldots, p_r$ are distinct primes, and $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$, and this expression is unique up to reordering the factors.

Justify your answers carefully.

(1) Using prime factorizations or otherwise, compute the greatest common divisors of the following pairs of integers.

(a) $10!$, 6^5.

(b) 84^{10}, 90^7.

(2) Compute the number of positive integers $d \in \mathbb{N}$ such that $d \mid 72^{100}$.

(3) Suppose a and b are positive integers and $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ and $b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$ are their prime factorizations. Determine a condition on the two prime factorizations that is equivalent to $\gcd(a, b) = 1$.

(4) Find all solutions $x, y \in \mathbb{Z}$ of each of the following equations.

(a) $91x + 133y = 52$.

(b) $57x + 78y = 6$.

(5) (a) Find all solutions $x, y \in \mathbb{Z}$ of the equation $13x + 17y = 250$.

(b) Using part (a) or otherwise, find all solutions $x, y \in \mathbb{Z}$ of the equation $13x + 17y = 250$ such that $x \geqslant 0$ and $y \geqslant 0$.

(6) Find all solutions of the congruence $57x \equiv 6 \bmod 123$.

(7) The goal of this question is to convince you that the uniqueness statement in the fundamental theorem of arithmetic is not obvious and needs to be proved carefully.

Consider the set

$$S = \{n \in \mathbb{N} \mid n \equiv 1 \bmod 4\} = \{1, 5, 9, 13, \ldots\}.$$

We say an element $n \in S$ is a *pseudoprime* if $n \neq 1$ and the only elements of S which divide n are 1 and n.

(a) Write down all the pseudoprimes which are less than 100. [Hint: There are 25 elements of S less than 100 and 19 of these are pseudoprimes.]

(b) Show that if $a \in S$ and $b \in S$ then $ab \in S$.

(c) Suppose $n, d \in \mathbb{N}$ and $d \mid n$, that is, $n = qd$ for some $q \in \mathbb{Z}$. Show that if $d \in S$ and $n \in S$ then $q \in S$.

(d) Using part (c), prove the following statement by strong induction: For all $n \in S$, n can be expressed as a product of pseudoprimes.

(e) Find an element $n \in S$ which can be expressed as a product of pseudoprimes in two different ways. (Here we regard two factorizations as the same if one is obtained from the other by reordering the factors.)

(8) We say a positive integer n is a *perfect square* if there is a positive integer m such that $n = m^2$.

(a) Prove the following statement: For all positive integers n, n is a perfect square if and only if in the prime factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ of n all the exponents $\alpha_1, \alpha_2, \ldots, \alpha_r$ are even.

(b) Using part (a), give a proof by contradiction of the following result: If $n \in \mathbb{N}$ is not a perfect square then $\sqrt{n}$ is irrational.

[Remark: Earlier we proved $\sqrt{2}$ and $\sqrt{3}$ are irrational. This is a more general result whose proof depends on the fundamental theorem of arithmetic.]

(9) Let

$$R = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\},$$

a subset of the complex numbers. Note that for all $\alpha, \beta \in R$, we have $\alpha + \beta \in R$ and $\alpha\beta \in R$. The operations of addition and multiplication make R into an algebraic structure called a *ring* (similar to the ring of integers $\mathbb{Z}$). The elements of R are called *Gaussian integers.* There is an analogue of the fundamental theorem of arithmetic for the Gaussian integers. We won't prove this here, but we will study the relation between primes in $\mathbb{Z}$ and primes in R.

(a) For a Gaussian integer $\alpha = a + bi$ we define the *norm* $N(\alpha)$ of α by $N(\alpha) = N(a + bi) = a^2 + b^2$. Prove that for all $\alpha, \beta \in R$ we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

(b) We say $\alpha \in R$ is a *unit* if there exists $\beta \in R$ such that $\alpha\beta = 1$. Using part (a), show that if α is a unit then $N(\alpha) = 1$. Deduce that the units in R are $1, -1, i$, and $-i$.

For $\alpha, \beta \in R$, we say α *divides* β and write $\alpha \mid \beta$ if there is a Gaussian integer $\gamma \in R$ such that $\beta = \gamma\alpha$. We say $\alpha \in R$ is a *Gaussian prime* if the only Gaussian integers which divide α are ± 1, $\pm i$, $\pm\alpha$, and $\pm i\alpha$.

[Remark: The units $\pm 1, \pm i$ in R play the same role as the units ± 1 in $\mathbb{Z}$. (In fact, when we defined primes in $\mathbb{Z}$, we restricted our attention to positive integers and so did not need to consider the divisors -1 and $-p$ of a prime number p.)]

(c) Using the identity $(a + bi)(a - bi) = a^2 + b^2$ or otherwise, prove that $2, 5, 13$ and 17 are *not* Gaussian primes.

[Remark: In fact it is a theorem of Fermat that for any prime $p \in \mathbb{N}$ such that $p \not\equiv 3 \bmod 4$ there exist positive integers $a, b \in \mathbb{N}$ such that $p = a^2 + b^2$. It follows that p is not a Gaussian prime (why?).]

(d) Suppose $p \in \mathbb{N}$ is a prime and that $p \equiv 3 \bmod 4$. Give a proof by contradiction that p is a Gaussian prime.

[Hint: Suppose that $\alpha \in R$ divides p and $\alpha \neq \pm 1, \pm i, \pm p, \pm ip$. Write $p = \alpha\beta$ for some $\beta \in R$. Using part (a) we find $p^2 = N(p) = N(\alpha)N(\beta)$. Show that $N(\alpha) \neq 1$ and $N(\beta) \neq 1$, so that we must have $N(\alpha) = N(\beta) = p$ (why?). Finally show that there do *not* exist integers a and b such that $a^2 + b^2 \equiv 3 \bmod 4$ and use this to obtain a contradiction.].