Math 300.3 Homework 8

Paul Hacking

March 29, 2017

Reading: Sundstrom, Sections 8.2 and 8.3.

Recall the fundamental theorem of arithmetic: Every positive integer n such that $n \neq 1$ 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 $r \in \mathbb{N}$, $p_1, p_2, \ldots, p_r$ 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) Compute the number of positive integers $d \in \mathbb{N}$ such that $d \mid 72^{100}$.

(2) 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 $\gcd(a, b) = 1$.

(3) (a) Prove the following statement: For all $n \in \mathbb{N}$, n is congruent to the sum of its digits modulo 9.

(b) Is 12345678987654321 divisible by 9? Justify your answer carefully.

(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) 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 such that $n \neq 1$, n is a perfect square if and only if in the prime factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ 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: For all $n \in \mathbb{N}$, if 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.]

(7) Dirichlet's theorem on primes in arithmetic progressions is the following result: For all $a, b \in \mathbb{N}$ such that $\gcd(a, b) = 1$, the arithmetic progression

$$\{na + b \mid n \in \mathbb{Z}, n \geqslant 0\} = \{b, a + b, 2a + b, 3a + b, \ldots\}$$

contains infinitely many prime numbers.

The proof of Dirichlet's theorem requires advanced techniques and is outside the scope of this course. In this question we will give an elementary proof of the special case $a = 4$ and $b = 3$.

(a) Prove the following statement: For all $a, b \in \mathbb{N}$, if $\gcd(a, b) \neq 1$ then the arithmetic progression

$$\{b, a + b, 2a + b, 3a + b, \ldots\}$$

contains at most one prime.

(b) Prove the following statement: For all $m \in \mathbb{N}$, if m is odd then either $m \equiv 1 \bmod 4$ or $m \equiv 3 \bmod 4$.

(c) Prove the following statement by induction: For all $a_1, \ldots, a_r \in \mathbb{Z}$, if $a_i \equiv 1 \bmod 4$ for $i = 1, 2, \ldots, r$ then $a_1 a_2 \cdots a_r \equiv 1 \bmod 4$.

(d) Now give a proof by contradiction that there are infinitely many primes p such that $p \equiv 3 \bmod 4$ (equivalently, $p = 4n+3$ for some $n \in \mathbb{Z}$ such that $n \geqslant 0$) as follows. Suppose that there are only finitely many primes p such that $p \equiv 3 \bmod 4$, and let $p_1, p_2, \ldots, p_s$ be the list of all such primes. Now consider the number

$$N = 4p_1p_2 \cdots p_s - 1.$$

Show that N must have a prime factor p such that $p \equiv 3 \bmod 4$ (using the hint below and part (c)), and use this to obtain a contradiction.

[Hint: Recall (see HW4Q2a) that if p is a prime then either $p = 2$ or p is odd. So, combining with part (b), if p is a prime then either $p = 2$ or $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$.]

(8) 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*.

(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 $\alpha \in R$ such that $\alpha \neq 0$ and $\beta \in R$, 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.].