Solutions to the Second Assignment
Basic Algebra

September 24, 2004

Solution of the problem 1. It need not be the case. Here are two counterexamples: $a = 2,\ b = c = 1$; or $a = 5,\ b = 2,\ c = 3$.

Solution of the problem 2. Here are again two counterexamples: $a = 6,\ b = 2,\ c = 3$; or $a = 9,\ b = 6,\ c = 15$.
Remark The statement will be true if we assume that a is a prime in $\mathbb{Z}$.

Solution of the problem 3. First of all, it is readily seen that $R = \{a + b\sqrt{-5} :\ a, b \in \mathbb{Z}\}$, usually denoted by $\mathbb{Z}[\sqrt{-5}]$, with usual addition and multiplication of complex numbers, is a ring whose identity element is 1. Also let us recall that in any ring R with identity element 1_R, an element α is called a *unit* if $\alpha\beta = 1_R$ for some β in R. We now identify all the units in $\mathbb{Z}[\sqrt{-5}]$.

To do this, it is useful to introduce the norm of an element. For $\alpha = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, the *norm* of α is defined by $N(\alpha) = a^2 + 5b^2 = \alpha\bar{\alpha}$, where $\bar{\alpha}$ is the usual complex conjugate of α. The norm function enjoys the following properties:

(1) $N(\alpha) \in \{0, 1, 2, 3, \cdots\}$; and $N(\alpha) = 0$ iff $\alpha = 0$.

(2) α is a unit iff $N(\alpha) = 1$ iff $\alpha = \pm 1$.

(3) $\alpha \mid \beta$ implies $N(\alpha) \mid N(\beta)$. Note that the first divisibility is in $\mathbb{Z}[\sqrt{-5}]$, whoever, the second one is in $\mathbb{Z}$.

We shall now show that $p = 3$ is *irreducible* in $\mathbb{Z}[\sqrt{-5}]$, i.e., its only divisors are $\pm 1,\ \pm 3$. To see this, assume that $\beta \mid \alpha$. So $\alpha = \beta\gamma$ for some γ. Taking the norms of both sides, we deduce that $9 = N(\beta)N(\gamma)$. If $N(\beta) = 1$, namely if β is a unit, we are done. Likewise we are on the safe side if $N(\gamma) = 1$. Thus suppose that $N(\beta) = N(\gamma) = 3$. Writing $\beta = a + b\sqrt{-5}$, this is equivalent to $a^2 + 5b^2 = 3$, which is impossible for $a, b \in \mathbb{Z}$. This concludes the assertion.

For the second part of the problem, note that

$$3 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

However, 3 divides neither $1 + \sqrt{-5}$ nor $1 - \sqrt{-5}$. For assume that for example $3 \mid 1 + \sqrt{-5}$, so $1 + \sqrt{-5} = 3(c + d\sqrt{-5})$. This in turn implies that $3c = 3d = 1$ which is absurd in $\mathbb{Z}$.

Remark All these show that $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.

Solution of the problem 4. First of all notice that $1 < 2 \leq 1! + 1$, and $2 < 3 \leq 2! + 1$. So, we actually don't need to require that n be > 2. Let us now recall the following well-known fact:

Every $m > 1$ has a prime divisor.

We now proceed the proof. By the above fact, it will suffice to show that no prime $p \leq n$ can divide $m = n! + 1$. So, suppose that $p \leq n$. Therefore $p \mid 1 \times 2 \times \cdots \times p \times \cdots \times n = n!$. Now if $p \mid n! + 1$, then it has to divide $(n! + 1) - n! = 1$, which is a contradiction.

To conclude that there are infinitely many primes, note that if we had only a finite number of them, and if p were the largest one, then by what we have shown above, there would be a prime $p < q \leq p! + 1$, which is nonsense.

Solution of the problem 5. Let $p_1 = 2, p_2 = 3, \cdots, p_k$ be the complete list of all primes $\leq N$, and let n be an N-smooth number. Thus $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, for some nonzero α_i's, and note that this factorization is unique by Fundamental Theorem of Arithmetic. Now let us recall that for $-1 < x < 1$,

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots.$$

So, for any prime number p, since $0 < \frac{1}{p} < 1$, we have

$$\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots.$$

Therefore,

$$\begin{aligned} \prod_{p \leq N} \frac{1}{1-\frac{1}{p}} &= \prod_{i=1}^{k} \frac{1}{1-\frac{1}{p_i}} \\ &= \prod_{i=1}^{k} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots\right). \end{aligned}$$

Now if we expand the right-hand side, we obtain all the fractions of the form $\frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}$, where α_i's are ≥ 0. What we get is in fact the sum of reciprocals of all N-smooth numbers. Hence

$$\prod_{p \leq N} \frac{1}{1-\frac{1}{p}} = \sum_{\substack{\text{all } N\text{-smooth} \\ n'\text{s}}} \frac{1}{n}.$$

Solution of the problem 6. Let us write

$$S_N := \prod_{p \leq N} \frac{1}{1-\frac{1}{p}}.$$

¿From the previous problem we know that $S_N = \sum_{\substack{\text{all } N-\text{smooth} \\ n'\text{s}}} \frac{1}{n}$. On the other hand, since any $n \leq N$ is clearly N-smooth, so we immediately deduce that

$$S_N \geq \sum_{n \leq N} \frac{1}{n}.$$

Now taking the limit when $N \to \infty$ and observing that the sum on the right-hand sude of the above inequality is in fact the N-th partial sum of the harmonic series (which is divergent), we infer that

$$\lim_{N \to \infty} \left(\prod_{p \leq N} \frac{1}{1 - \frac{1}{p}} \right) = \lim_{N \to \infty} S_N = \infty.$$

Solution of the problem 7. If we take the natural logarithm of S_N, and if we use the well-know expansion

$$\log \frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots, \qquad -1 < x < 1$$

we deduce that

$$\begin{aligned}
\log S_N &= \log \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}} \\
&= \sum_{p \leq N} \log \frac{1}{1 - \frac{1}{p}} \\
&= \sum_{p \leq N} \left(\frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \cdots \right) \\
&= \sum_{p \leq N} \frac{1}{p} + \sum_{p \leq N} \left(\frac{1}{2p^2} + \frac{1}{3p^3} + \cdots \right). \qquad (\star)
\end{aligned}$$

However, the very last sum is bounded above:

$$\begin{aligned}
\sum_{p \leq N} \left(\frac{1}{2p^2} + \frac{1}{3p^3} + \cdots \right) &\leq \sum_{p \leq N} \left(\frac{1}{p^2} + \frac{1}{p^3} + \cdots \right) \\
&\leq \sum_{\text{all } p'\text{s}} \left(\frac{1}{p^2} + \frac{1}{p^3} + \cdots \right) \\
&= \sum_{\text{all } p'\text{s}} \frac{1}{p(p-1)} \\
&\leq \sum_{\text{all } n \geq 2} \frac{1}{n(n-1)} \\
&= 1.
\end{aligned}$$

Now if N tends to ∞, then S_N will go to ∞, so does $\log S_N$ as well. So the right-hand side of $(\star)$ has infinite limit when $N \to \infty$, and since the second sum in $(\star)$ has a finite contribution, we conclude that

$$\sum_{\text{all } p'\text{s}} \frac{1}{p} = \lim_{N \to \infty} \sum_{p \leq N} \frac{1}{p} = \infty.$$