Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 20, 2020

Problems in Section 3.8.

1. Find all the units in $J[i]$.

Proof. Since $J[i]$ is an Euclidean ring, $a = p + qi \in J[i]$ is an unit if and only if $d(a) = d(1)$. Equivalently, $d(a) = d(1) \iff p^2 + q^2 = 1$ so that there are 4 units, namely: $1, -1, i, -i$. □

2. If $a + bi$ is not a unit of $J[i]$ prove that $a^2 + b^2 > 1$.

Proof. It follows directly from Problem 1. □

3. Find the greatest common divisor in $J[i]$ of
a) $3 + 4i$ and $4 - 3i$.

Solution. Note that

$$3 + 4i = i(4 - 3i)$$

so that the greatest common divisor of $3 + 4i$ and $4 - 3i$ is $3 + 4i$. □

b) $11 + 7i$ and $18 - i$.

Solution. Note that

$$\begin{aligned}
&18 - i = 1(11 + 7i) + (7 - 8i), \\
&11 + 7i = i(7 - 8i) + 3, \\
&7 - 8i = (2 - 3i)3 + (1 + i), \\
&3 = (1 - 2i)(1 + i) + i, \\
&1 + i = 1 \cdot i + 1, \\
&i = i \cdot 1
\end{aligned}$$

so that the greatest common divisor of $11 + 7i$ and $18 - i$ is 1. □

4. Prove that if p is a prime number of the form $4n+3$, then there is no x such that $x^2 \equiv -1 \bmod p$.

Proof. Suppose there is x satisfying $x^2 \equiv -1 \bmod p$. We know that by Fermat's Little Theorem, $x^p \equiv x \iff x^{4n+3} \equiv x \bmod p$. As $x^4 \equiv 1 \bmod p$, $x^3 \equiv x \bmod p$ so that $x^2 \equiv 1 \bmod p$, which is a contradiction. Therefore, there is no prime number of form $4n+3$ with x satisfying $x^2 \equiv -1 \bmod p$. $\square$

5. Prove that no prime of the form $4n+3$ can be written as a^2+b^2 where a and b are integers.

Proof. In fact, there is no integer of form $4n+3$ can be written as sum of two squares. We divide into four cases:

- (Case 1) a and b are even. We have $a = 2k, b = 2l$ so that $a^2+b^2 = 4(k^2+l^2) \equiv 0 \pmod 4$.
- (Case 2) a and b are odd. We have $a = 2k+1, b = 2l+1$ so that $a^2+b^2 = 4(k^2+k+l^2+l)+2 \equiv 2 \pmod 4$.
- (Case 3) either a or b is odd: We have $a = 2k, b = 2l+1$ so that $a^2+b^2 = 4(k^2+l^2+l)+1 \equiv 1 \pmod 4$.

So in either cases, $a^2+b^2 \not\equiv 3 \pmod 4$. $\square$

6. Prove that there is an infinite number of primes of the form $4n+3$.

Proof. Suppose there are only finitely many primes of the form $4n+3$ $p_1 = 3, p_2, \cdots, p_k$. Consider $q = 4p_2p_3\cdots p_k + 3$. Note that $q \equiv 3 \pmod 4$. But no p_i's divide q so that q admits only primes of the form $4n+1$ as a divisor. But note that product of integers of form $4n+1$ is again the same, so that is a contradiction that q is an integer of the form $4n+3$. Hence there must be infinite number of primes of the form $4n+3$. $\square$

7. Prove that there exists an infinite number of primes of the form $4n+1$.

Proof. Suppose there are only finitely many primes of the form $4n+1$ $p_1, p_2, \cdots, p_k$. Consider $q = (2p_1p_2\cdots p_k)^2+1$. Note that for any odd prime p dividing q is not a form of $4n+3$. For such p, $2p_1p_2\cdots p_k$ is a solution for the congruence equation $x^2 \equiv -1 \pmod p$. But this forces that p is not a form of $4n+3$ so that $p = p_i$ for some i, which is a contradiction. Hence there must be an infinite number of primes of the form $4n+1$. $\square$

8. Determine all the prime elements in $J[i]$.

Solution. We prove the following: $a+bi \in J[i]$ is prime if and only if a^2+b^2 is prime in J. Suppose $a+bi$ is a prime in $J[i]$. Note that $a^2+b^2=(a+bi)(a-bi)$. If a^2+b^2 is a prime, then we are done. If not, since $J[i]$ is an Unique Factorization Domain, the two prime factors of a^2+b^2 must be associates of $a+bi$ and $a-bi$ respectively. Since $a+bi$ being an associate with a prime element in J, $ab=0$. Conversely, assume that a^2+b^2 is a (positive integer) prime in J. Suppose $a+bi=(c+di)(e+fi)$. We know that $a^2+b^2=(c^2+d^2)(e^2+f^2)$. Thus, either $c^2+d^2=1$ or $e^2+f^2=1$ so that, equivalently, either $c+di$ or $e+fi$ is an unit in $J[i]$. This proves that $a+bi$ is a prime(irreducible) in $J[i]$. □

9. Determine all positive integers which can be written as a sum of two squares(of integers).

Proof. We claim that a positive integer can be written as a sum of two squares if and only if its prime divisors of form $4k+3$ occur within even powers. Let $n=m^2r$ where m^2 is the largest square divisor so that r is square free. Suppose $r=1$. Then $n=m^2+0^2$, so we are done. Thus we assume that $r>1$. If $r=2$, $n=2m^2=m^2+m^2$. From our assumption, if $r>2$, r has prime divisors of forms $4k+1$ only. Thus, r is expressible as product of sum of integers of two squares of integers. But since product of sum of two squares is again a sum of two squares, n is again a product of sum of two squares so that, in ultimately, n is the sum of two squares.
Conversely, suppose that n can be written as a sum of two squares, that is, $n=m^2r=a^2+b^2$. Let $(a,b)=d$. Then $a_0d=a, b_0d=b$ where $(a_0,b_0)=1$. Thus, $m^2r=d^2(a_0^2+b_0^2)$. Since r is square free, $d \mid m$ so that $dm'=m \implies (m')^2r=a_0^2+b_0^2$. Now for the sake of contradiction, assume that r has a prime divisor p of form $4k+3$. Then

$$a_0^2+b_0^2 \equiv 0 \pmod{p} \iff a_0^2 \equiv -b_0^2 \pmod{p}.$$

If $p \nmid a_0, p \nmid b_0$ otherwise $(a_0,b_0) \neq 1$. Thus, $(a_0,p)=(b_0,p)=1$. Now by Fermat's Little Theorem,

$$\begin{aligned}
&a_0^{p-1} \equiv 1, b_0^{p-1} \equiv 1 \pmod{p},\\
\implies &a_0^{4k+2} \equiv b_0^{4k+2} \pmod{p},\\
\implies &a_0^{4k} \equiv b_0^{4k}(-1) \pmod{p},\\
\implies &1 \equiv -1 \pmod{p},
\end{aligned}$$

which is clearly a contradiction. Hence, proved. □