ALGEBRA HW 7

CLAY SHONKWILER

1

Prove, or disprove and salvage: If K is a field, and $f(x) \in K[x]$ has no roots, then $K[x]/(f(x))$ is a field.

Counter-example: Consider the field $K = \mathbb{Q}$ and the polynomial

$$f(x) = x^4 + 3x^2 + 2.$$

Then $f(x) = (x^2 + 1)(x^2 + 2)$, which has roots $\pm i, \pm 2i$, none of which, certainly, is in $\mathbb{Q}$. However, since $f(x)$ is reducible (with the factorization just given), we know that $(f(x))$ is not a maximal ideal and, thus, that $\mathbb{Q}/(f(x))$ is not a field.

To salvage this claim, let us consider only polynomials $f \in K[x]$ for some field K that are of degree 2 or 3. Then, if f has no roots in K, then $K[x]/(f(x))$ is a field. To see why, note that, since f has degree 2 or 3, f must have a linear factor if f is reducible. However, a linear factor $x - a$ has a as a root so, if f has no roots in K, f cannot be factored in $K[x]$ by a linear factor. Hence, we conclude that such an f is irreducible and, thus, that $(f(x))$ is maximal, so $K[x]/(f(x))$ is a field.

♣

2

For each positive integer n, let $U_n = (\mathbb{Z}/n)^*$, the group of units modulo n. Find a generator of U_{121}, and determine the group structure of U_{27} and U_{21} explicitly. Conjectures? Proofs?

Answer: The units of $\mathbb{Z}/121$ will be precisely those integers less than 121 that are relatively prime to 121; hence, since $121 = 11^2$, the non-units of $\mathbb{Z}/121$ are simply the multiples of 11. Since there are 11 such (namely 0, 11, 22, 33, 44, 55, 66, 77, 88, 99, 110), the order of U_{121} is $121 - 11 = 110$. Now, consider $2 \in U_{121}$. Now, the possible orders of any element in U_{121} are $2, 5, 10, 11, 22, 55$. Now,

$$\begin{aligned}
2^2 &= 4 \equiv 4 \mod 121 \\
2^5 &= 32 \equiv 32 \mod 121 \\
2^{10} &= 1024 \equiv 56 \mod 121 \\
2^{11} &= 2 \cdot 2^{10} \equiv 2 \cdot 56 \equiv 112 \mod 121 \\
2^{22} &= 2^{11} \cdot 2^{11} \equiv 112 \cdot 112 \equiv -9 \cdot -9 \equiv 81 \mod 121 \\
2^{55} &= (2^{11})^5 \equiv (-9)^5 = -59049 \equiv -1 \mod 121.
\end{aligned}$$

Hence, we see that the order of 2 in U_{121} must be 110, so 2 generates U_{121}.

Note that the non-units in $\mathbb{Z}/27$ are precisely the multiples of 3; since there are 9 such, we see that $\#(U_{27}) = 18$. Now,

$$\begin{aligned} 2 \cdot 2 &= 4 \equiv 4 \mod 27 \\ 2 \cdot 4 &= 8 \equiv 8 \mod 27 \\ 2 \cdot 8 &= 16 \equiv 16 \mod 27 \\ 2 \cdot 16 &= 32 \equiv 5 \mod 27 \\ 2 \cdot 5 &= 10 \equiv 10 \mod 27 \\ 2 \cdot 10 &= 20 \equiv 20 \mod 27 \\ 2 \cdot 20 &= 40 \equiv 13 \mod 27 \\ 2 \cdot 13 &= 26 \equiv -1 \mod 27, \end{aligned}$$

so we see that $2 \in U_{27}$ has order 18, so we see that $U_{27} \simeq C_{18}$.

Note that the non-units of $\mathbb{Z}/21$ are the multiples of 3 and 7; namely 0, 3, 6, 7, 9, 12, 14, 15, 18. There are 9 such, so we see that $\#(U_{21}) = 12$. Now, U_{21} is certainly abelian, so either $U_{21} \simeq C_{12}$ or $U_{21} \simeq C_2 \times C_6$. Now,

$$\begin{aligned} 2 \cdot 2 &= 4 \equiv 4 \mod 21 \\ 2 \cdot 4 &= 8 \equiv 8 \mod 21 \\ 2 \cdot 8 &= 16 \equiv 16 \mod 21 \\ 2 \cdot 16 &= 32 \equiv 11 \mod 21 \\ 2 \cdot 11 &= 22 \equiv 1 \mod 21 \\ 13 \cdot 13 &= 169 \equiv 1 \mod 21 \\ 2 \cdot 13 &= 26 \equiv 5 \mod 21 \\ 2 \cdot 5 &= 10 \equiv 10 \mod 21 \\ 2 \cdot 10 &= 20 \equiv 20 \mod 21 \\ 13 \cdot 11 &= 143 \equiv 17 \mod 21 \\ 13 \cdot 16 &= 208 \equiv 19 \mod 21; \end{aligned}$$

hence, we see that 2 has order 6 and 13 has order 2 and that, furthermore, $U_{21} = \langle 2, 13 \rangle$, which is to say that $U_{21} \simeq C_2 \times C_6$.

Conjecture: If p prime, then $U_{p^k} \simeq C_{p^k - p^{k-1}}$. If m and n are relatively prime, then $U_{mn} \simeq U_m \times U_n$.

Proof. Of second part. If m, n relatively prime, define

$$f : U_{mn} \to U_m \times U_n$$

by

$$f(x) = (x, x)$$

where we interpret the terms on the right modulo m and n, respectively. Then, for $x, y \in U_{mn}$,

$$f(xy) = (xy, xy) = (x, x)(y, y),$$

so f is a homomorphism. If $x, y \in U_{mn}$ such that $f(x) = f(y)$, then

$$(x, x) = (y, y)$$

implies $x \equiv y \mod m$ and $x \equiv y \mod n$. Hence, there exist i, j such that $x = y + im$ and $x = y + jn$. Thus, $y + im = y + jn$, so $im = jn$ is a

common multiple of m and n. Since m and n are relatively prime, their l.c.m. is mn; since the l.c.m. generates all multiples, there exists k such that $im = k(mn) = jn$, so

$$\begin{aligned} x &= y + im = y + k(mn) \\ x &= y + jn = y + k(mn). \end{aligned}$$

That is to say, $x \equiv y \mod mn$, so $x = y$ in U_{mn}. Thus, f is injective.

On the other hand, if $(a, b) \in U_m \times U_n$, then, by the Chinese Remainder Theorem, there exists $x \in \mathbb{Z}$ such that $x \equiv a \mod m$ and $x \equiv b \mod n$; hence, $f(x) = (a, b)$, so f is surjective. Therefore, we conclude that f is an isomorphism. □

♣

3

(a): Define the Euclidean algorithm as follows. Given non-zero integers a and b, write $a = bq_0 + r_0$ as in the division algorithm (i.e. $0 \leq r_0 \leq |b|$); then continue: $b = r_0q_1 + r_1$, $r_1 = r_2q_3 + r_3$, etc. (with $0 \leq r_{i+1} \leq |r_i|$). Show that eventually some $r_{n+1} = 0$, and that r_n is the g.c.d. of a and b.

Proof. Note that $\langle |r_i| \rangle$ is a descending sequence of non-negative integers; since there are no infinite descending chains in $\mathbb{N}$, we see that $r_k = 0$ for some $k \in \mathbb{N}$. Let $n + 1$ be the least integer such that $r_{n+1} = 0$. Then r_n, r_{n-1} are non-zero and

$$r_{n-1} = r_nq_{n+1} + r_{n+1} = r_nq_{n+1},$$

so we see that $r_n | r_{n-1}$. Now, suppose $r_n | r_i$ for all $i > j$. Then

$$r_j = r_{j+1}q_{n+2} + r_{j+2};$$

since $r_n | r_{j+1}$ and $r_n | r_{j+1}$, we can factor r_n from the right side, which guarantees that $r_n | r_j$. Hence, by induction, $r_n | r_i$ for all $0 \leq i \leq n$. Hence, since

$$b = r_0q_1 + r_1,$$

$r_n | b$. Further, since

$$a = bq_0 + r_0,$$

$r_n | a$, so we see that r_n is a common divisor of a and b. Since (a, b) is principal and is generated by the greatest common divisor of a and b, if $r_n \in (a, b)$, then this suffices to show that r_n is the g.c.d. of a and b. To that end, note that

$$r_0 = a - bq_0 \in (a, b).$$

In general, if $r_i \in (a, b)$ for all $i < k$, then

$$r_k = r_{k-2} - r_{k-1}q_{k-2} \in (r_{k-2}, r_{k-1}) \subset (a, b),$$

so $r_k \in (a,b)$. Thus, by induction, we see that $r_i \in (a,b)$ for $0 \leq i \leq n$. Specifically, $r_n \in (a,b)$, so we conclude that r_n is the g.c.d. of a and b. □

(b): Use this to find the g.c.d. of 1155 and 651.

Answer: The steps described in (a) above lead to the following series of equations:

$$\begin{aligned} 1155 &= (651)(1) + 504 \\ 655 &= (504)(1) + 147 \\ 504 &= (147)(3) + 63 \\ 147 &= (63)(2) + 21 \\ 63 &= (21)(3) + 0 \end{aligned}$$

so we see that the g.c.d. of 1155 and 651 is 21.

♣

(c): Verify, in the calculations of part (b), that (in the notation of (a)),

$$\frac{1155}{651} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_n}}}}$$

Also verify in these calculations that if we write

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_{n-1}}}}} = \frac{x}{y}$$

in lowest terms, then x, y form a solution to the Diophantine equation $651x - 1155y = d$, where $d = \gcd(1155, 651)$. Can solutions to other equations be found in this way? Explore.

Proof. Note that

$$\begin{aligned} 1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2 + \frac{1}{3}}}} &= 1 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{1}{\frac{7}{3}}}} \\ &= 1 + \cfrac{1}{1 + \frac{1}{\frac{24}{7}}} \\ &= 1 + \frac{1}{\frac{31}{24}} \\ &= 1 + \frac{24}{31} \\ &= \frac{55}{31} \\ &= \frac{1155}{651} \end{aligned}$$

Now, turning to the second equation,

$$\begin{aligned} 1 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{1}{2}}} &= 1 + \cfrac{1}{1 + \frac{1}{\frac{7}{2}}} \\ &= 1 + \frac{1}{\frac{9}{7}} \\ &= \frac{16}{9} \end{aligned}$$

and

$$651(16) - 1155(9) = 10,416 - 10,395 = 21 = \gcd(651, 1155).$$

In general, consider the Diophantine equation $ax + by = d$, where d is the g.c.d. of a and b. Then we can use the Euclidean algorithm to find d and, traversing backwards, we see that, since $d = r_n$ and $r_{i+2} = r_i - r_{i+1}q_{i+2}$,

$$\begin{aligned} d = r_n &= r_{n-2} - r_{n-1}q_n \\ &= r_{n-2} - [r_{n-3} - r_{n-2}q_{n-1}]q_n \\ &= r_{n-3}q_n + r_{n-2}[1 + q_{n-1}q_n] \\ &= r_{n-3}q_n + [r_{n-4} - r_{n-3}q_{n-2}][1 + q_{n-1}q_n] \\ &= r_{n-4}[1 + q_{n-1}q_n] + r_{n-3}[q_n - q_{n-2}(1 + q_{n-1}q_n] \\ &\vdots \\ &= ar + br' \end{aligned}$$

for r, r' in terms of the r_i's and q_j's. This procedure *always* gives a solution of the Diophantine Equation $ax + by = d$ where d is the g.c.d. of a and b.

□

4

Do the analog of problem 3 with $\mathbb{Z}$ replaced by $k[x]$, where k is a field. In parts (b) and (c), replace 1155 and 651 with $x^3 + x^2 + x$ and $x^2 + 1$.

(a): Given $f(x), g(x) \in k[x]$, define the algorithm given by

$$\begin{aligned} f(x) &= g(x)q_0(x) + r_0(x) \\ g(x) &= r_0(x)q_1(x) + r_1(x) \\ r_0(x) &= r_1(x)q_2(x) + r_2(x) \\ &\vdots \end{aligned}$$

where $r_i \equiv 0$ or $\deg(r_i) < \deg(r_{i-1})$. Then $\deg(r_i)$ is a decreasing sequence of non-negative integers, so it must reach zero in finitely many steps. Let $n+1$ be the smallest integer such that $\deg(r_{n+1}) = 0$. Then

$$r_{n-1}(x) = r_n(x)q_{n+1}(x) + r_{n+1}(x) = r_n(x)q_{n+1}(x),$$

so we see that $r_n(x)|r_{n-1}(x)$. Now, suppose $r_n(x)|r_i(x)$ for all $i > j$. Then

$$r_j(x) = r_{j+1}(x)q_{n+2}(x) + r_{j+2}(x);$$

since $r_n(x)|r_{j+1}(x)$ and $r_n(x)|r_{j+1}(x)$, we can factor $r_n(x)$ from the right side, which guarantees that $r_n(x)|r_j(x)$. Hence, by induction, $r_n(x)|r_i(x)$ for all $0 \leq i \leq n$. Hence, since

$$g(x) = r_0(x)q_1(x) + r_1(x),$$

$r_n(x)|g(x)$. Further, since

$$f(x) = b(x)q_0(x) + r_0(x),$$

$r_n(x)|f(x)$, so we see that $r_n(x)$ is a common divisor of $f(x)$ and $g(x)$. Since $(f(x), g(x))$ is principal and is generated by the greatest

common divisor of $f(x)$ and $g(x)$, if $r_n(x) \in (f(x), g(x))$, then this suffices to show that $r_n(x)$ is the g.c.d. of $f(x)$ and $g(x)$. To that end, note that

$$r_0(x) = f(x) - g(x)q_0(x) \in (f(x), g(x)).$$

In general, if $r_i(x) \in (f(x), g(x))$ for all $i < k$, then

$$r_k(x) = r_{k-2}(x) - r_{k-1}(x)q_{k-2}(x) \in (r_{k-2}(x), r_{k-1}(x)) \subset (f(x), g(x)),$$

so $r_k(x) \in (f(x), g(x))$. Thus, by induction, we see that $r_i(x) \in (f(x), g(x))$ for $0 \leq i \leq n$. Specifically, $r_n(x) \in (f(x), g(x))$, so we conclude that $r_n(x)$ is the g.c.d. of $f(x)$ and $g(x)$.

♣

(b): The steps described in (a) above yield the following sequence of equations:

$$\begin{aligned} x^3 + x^2 + x &= (x^2 + 1)(x + 1) - 1 \\ x^2 + 1 &= (-1)(-x^2 - 1) + 0 \end{aligned},$$

so we see that $x^3 + x^2 + x$ and $x^2 + 1$ are relatively prime.

♣

(c): Note that

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

Furthermore, in the second equation,

$$x + 1 = \frac{x + 1}{1}$$

and

$$(x^2 + 1)(x + 1) - (x^3 + x^2 + x)(1) = 1 = \gcd(x^2 + 1, x^3 + x^2 + x).$$

Now, in our demonstration in 3(c) that this general procedure will solve equations of the form $ax + by = d$ did not depend on any properties of the integers other than the fact that we can do the Euclidean algorithm in $\mathbb{Z}$ and that $\mathbb{Z}$ is an integral domain. As such, the same argument demonstrates that we can use this procedure to find solutions of the equation $f(x)k(x)+g(x)l(x) = d(x)$, where $d(x)$ is the g.c.d. of $f(x)$ and $g(x)$.

♣

5

(a): Show that $\sqrt{2}$ is irrational.

Proof. Suppose $\sqrt{2} \in \mathbb{Q}$. Then there exist $a, b \in \mathbb{Z}$ such that $\frac{a}{b} = \sqrt{2}$ where a and b are relatively prime. Then

$$2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2},$$

or $a^2 = 2b^2 = (2b)b$. However, this implies that a is a multiple of b; since a and b are relatively prime, this is impossible. From this contradiction, then, we conclude that, in fact, $\sqrt{2}$ is irrational. □

(b): More generally, show that if $m \in \mathbb{Z}$ and $x^2 - m$ has no root in Z, then $x^2 - m$ has no root in $\mathbb{Q}$.

Proof. Suppose $x^2 - m$ has a root in $\mathbb{Q}$ but none in $\mathbb{Z}$. Then there exist $a, b \in \mathbb{Z}$ relatively prime such that

$$0 = \left(\frac{a}{b}\right)^2 - m = \frac{a^2}{b^2} - m \Rightarrow \frac{a^2}{b^2} = m.$$

Then $a^2 = mb^2 = (mb)b$, so a is a multiple of b; since a and b are relatively prime, this is impossible, so we conclude that there are no such a and b and, therefore, that $x^2 - m$ has no roots in $\mathbb{Q}$. □

(c): Still more generally, show that if $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$, and if the polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ has no root in $\mathbb{Z}$, then it has no root in $\mathbb{Q}$.

Proof. Suppose f has a root in $\mathbb{Q}$ but no roots in $\mathbb{Z}$. Then there exist $c, d \in \mathbb{Z}$ such that c and d are relatively prime and

$$\left(\frac{c}{d}\right)^n + a_{n-1}\left(\frac{c}{d}\right)^{n-1} + \ldots + a_1\left(\frac{c}{d}\right) + a_0 = 0.$$

Multiplying both sides by b^n, we see that

$$c^n + da_{n-1}c^{n-1} + \ldots + d^{n-1}a_1 c + d^n a_0 = 0.$$

Hence,

$$c^n = d(-a_{n-1}c^{n-1} - da_{n-2}c^{n-2} - \ldots - d^{n-2}a_1 c - d^{n-1}a_0),$$

so we see that $d|c^n$. However, since c and d are relatively prime, this is impossible. From this contradiction, then, we conclude that if f has no roots in $\mathbb{Z}$ then it has no roots in $\mathbb{Q}$. □

(d): What if, in part (c), the polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ (for some integers $a_0, a_1, \ldots, a_n$) is considered instead?

Answer: Clearly, the roots of the polynomial $9x^2 - 4$ are $x = \pm\frac{2}{3}$; namely, this polynomial has no roots in $\mathbb{Z}$ but does have roots in $\mathbb{Q}$. That having been said, there are conditions on the rational roots of such a polynomial. If

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

has rational root $\frac{c}{d} \in \mathbb{Q}$ such that $c, d \in \mathbb{Z}$ and c, d are relatively prime, then

$$a_n\left(\frac{c}{d}\right)^n + a_{n-1}\left(\frac{c}{d}\right)^{n-1} + \ldots + a_1\left(\frac{c}{d}\right) + a_0 = 0.$$

Thus, multiplying by b^n, we see that

$$a_n c^n + da_{n-1}c^{n-1} + \ldots + d^{n-1}a_1 c + d^n a_0 = 0.$$

Hence,

$$a_n c^n = -d(a_{n-1}c^{n-1} + da_{n-2}c^{n-2} + \ldots + d^{n-2}a_1 c + d^{n-1}a_0)$$

and

$$d^n a_0 = -c(a_n c^{n-1} + da_{n-1}c^{n-2} + \ldots + d^{n-2}a_2 c + d^{n-1}a_1).$$

Thus, $d|a_n c^n$ and $c|a^n a_0$; since c and d are relatively prime, we see that

$$d|a_n \text{ and } c|a_0.$$

This fact then puts significant restrictions on the possibilities for rational roots of such a polynomial.

♣

6

(a): Describe the maximal ideals in each of the following rings: $(\mathbb{Z}/2)[x]$, $\mathbb{C}[x,y,z,t]$, $\mathbb{R}[[x]]$, $\mathbb{Z}_{(2)}$, $\mathbb{Z}[1/15]$, $\mathbb{Z}/15$, $\mathbb{C}[x,y]/(y^2-x^3)$, $\mathbb{Q}[i]$, $\mathbb{R}\times\mathbb{R}$, $\mathbb{C}[x]/(x^2)$.

(b): Describe all the units in these rings. Which have only finitely many units?

7

Let p be a prime number and let n be a positive integer such that $p \equiv 1 \mod n$.

(a): Show that the map $\phi_n : (\mathbb{Z}/p)^* \to (\mathbb{Z}/p)^*$, given by $\phi_n(x) = x^n$, is exactly n-to-one.

Proof. Since $(\mathbb{Z}/p)^* \simeq C_{p-1}$, we know that $(\mathbb{Z}/p)^* = \langle a \rangle$ for some $a \in (\mathbb{Z}/p)^*$. Hence, for all $b \in (\mathbb{Z}/p)^*$, $b = a^m$ for some m. Further, $b^{p-1} = 1$ for all $b \in (\mathbb{Z}/p)^*$ and, since $p \equiv 1 \mod n$, $p-1$ is divisible by n. Now, note that

$$\phi_n(a^{\frac{k(p-1)}{n}}) = (a^{\frac{k(p-1)}{n}})^n = a^{k(p-1)} = (a^{p-1})^k = 1^k = 1.$$

Since $a^{\frac{k(p-1)}{n}}$ are distinct for $k = 1, \ldots, n$, we see that ϕ_n is at least n-to-one, since each of the n elements of the form $a^{\frac{k(p-1)}{n}}$ is in the kernel of ϕ_n.

On the other hand, if $b = a_j$ is in the kernel of ϕ_n, then

$$a^{p-1} = 1 = \phi_n(b) = b^n = (a^j)^n = a^{jn},$$

so $jn = k(p-1)$ for some integer k and, hence, $j = \frac{k(p-1)}{n}$. If $k = n + i$ for some $i \geq 0$, then

$$j = \frac{(n+i)(p-1)}{n} = (p-1) + \frac{i(p-1)}{n}$$

and so

$$a^j = a^{(p-1)+\frac{i(p-1)}{n}} = a^{p-1}a^{\frac{i(p-1)}{n}} = a^{\frac{i(p-1)}{n}},$$

so we see there are at most n elements in the kernel. Thus, $\#(\ker \phi_n) = n$, so ϕ_n is exactly n-to-one. □

(b): Deduce that there are exactly $\frac{p-1}{n}$ elements of $(\mathbb{Z}/p)^*$ that are nth powers.

Proof. Since $(\mathbb{Z}/p)^*/\ker \phi_n \simeq \text{Image } \phi_n$ and Image ϕ_n is exactly the set of nth powers in $(\mathbb{Z}/p)^*$, we see that

$$\#(\text{Image } \phi_n) = \#((\mathbb{Z}/p)^*/\ker \phi_n) = \frac{\#((\mathbb{Z}/p)^*)}{\#(\ker \phi_n)} = \frac{p-1}{n}.$$

Hence, there are exactly $\frac{p-1}{n}$ elements of $(\mathbb{Z}/p)^*$ that are nth powers. □

(c): What happens if instead the congruence hypothesis is dropped?

Answer: Let $d = (n, p-1)$. Let $m = n/d$. Then, if $b = a^j \in \ker \phi_n$,

$$a^{p-1} = 1 = \phi_n(b) = b^n = (a^j)^n = a^{jn},$$

so $jn = k(p-1)$ for some k. Thus, $j = \frac{k(p-1)}{n} = \frac{k}{m}\frac{p-1}{d}$. So $\frac{k}{m}$ is an integer i and $j = \frac{i(p-1)}{d}$. Obviously,

$$a^{\frac{(d+l)(p-1)}{d}} = a^{\frac{d(p-1)}{d} + \frac{l(p-1)}{d}} = a^{p-1}a^{\frac{i(p-1)}{d}} = a^{\frac{i(p-1)}{d}},$$

so there are at most d possible choices for i. On the other hand,

$$(a^{\frac{i(p-1)}{d}})^n = (a^{\frac{i(p-1)}{d}})^{md} = (a^{i(p-1)})^m = 1,$$

so $a^{\frac{i(p-1)}{d}} \in \ker \phi_n$ for all $i = 1, \ldots, d$. Hence, we conclude that $\ker \phi_n$ has order d, so ϕ_n is d-to-one and thus, by the same argument given in (b), there are $\frac{p-1}{d}$ elements of $(\mathbb{Z}/p)^*$ that are nth powers. ♣

8

(a): Which of the following elements of $\mathbb{Z}[i]$ can be factored non-trivially? For each one that can be, do so explicitly. $2, 3, 5, 7, 11, 13, 15, 3i, 5i, 2+i, 3+i$.

Answer: Let $N(a)$ denote the norm of $a \in \mathbb{Z}[i]$. Recall that in $\mathbb{C}$ (and, therefore, in $\mathbb{Z}[i] \subset \mathbb{C}$), $N(ab) = N(a)N(b)$. Furthermore, since $N(ab) = \sqrt{c}$ for some $c \in \mathbb{N}$, we see that $N(a)^2$ and $N(b)^2$ must divide c.

$2 = (1+i)(1-i) = 1 - i^2 = 2$, so we see that 2 can be factored non-trivially.

$N(3) = 3$ so, if $ab = 3$, $N(a)^2 9$ and $N(b)^2 9$. Since the only non-trivial factorization of 9 is $3 \cdot 3$, we see that $N(a)^2 = N(b)^2 = 3$ or

either a or b is a unit. In the latter case, the factorization is trivial. Furthermore, if $a = \alpha + \beta i$, then

$$3 = N(a)^2 = \alpha^2 + \beta^2;$$

since 3 is not the sum of any two squares, we see that this is impossible, so 3 can only be factored trivially.

$5 = (1 + 2i)(1 - 2i)$, so 5 can be factored non-trivially.

$N(7) = 7$, so, if $ab = 7$, $N(a)^2|49$ and $N(b)^2|49$. The only non-trivial factorization of 49 is as $7 \cdot 7$, so we see that either a or b is a unit or $N(a)^2 = N(b)^2 = 7$. However, if $a = \alpha + \beta i$, then

$$7 = N(a)^2 = \alpha^2 + \beta^2;$$

since 7 is not the sum of two squares, this is impossible, so 7 can only be factored trivially.

$N(11) = 11$, so, if $ab = 11$, $N(a)^2|121$ and $N(b)^2|121$. The only non-trivial factorization of 121 is as $11 \cdot 11$, so we see that either a or b is a unit or $N(a)^2 = N(b)^2 = 11$. However, if $a = \alpha + \beta i$, then

$$11 = N(a)^2 = \alpha^2 + \beta^2;$$

since 11 is not the sum of two squares, this is impossible, so 11 can only be factored trivially.

$13 = (2 + 3i)(2 - 3i)$, so 13 can be factored non-trivially.

$15 = 3 \cdot 5$, so 15 can be factored non-trivially.

$N(3i) = 3$, so, if $ab = 3i$, $N(a)^2|9$ and $N(b)^2|9$. The only non-trivial factorization of 9 is as $3 \cdot 3$, so we see that either a or b is a unit or $N(a)^2 = N(b)^2 = 3$. However, if $a = \alpha + \beta i$, then

$$3 = N(a)^2 = \alpha^2 + \beta^2;$$

since 3 is not the sum of two squares, this is impossible, so $3i$ can only be factored trivially.

$5i = (2 + i)(1 + 2i)$, so $5i$ can be factored non-trivially.

$N(2 + i) = \sqrt{5}$, so, if $ab = 2 + i$, then $N(a)^2N(b)^2 = 5$. Since 5 cannot be factored non-trivially, we see that either $N(a) = 1$ or $N(b) = 1$; either way, either a or b is a unit, so $2 + i$ cannot be factored non-trivially.

$3 + i = (1 + i)(2 - i)$, so $3 + i$ can be factored non-trivially.

♣

(b): Make a conjecture about which Gaussian integers can be factored non-trivially.

Conjecture: $a \in \mathbb{Z}[i]$ cannot be factored non-trivially if and only if either $N(a)$ is a prime congruent to 3 modulo 4 or $N(a) = \sqrt{b}$ for some prime b.

DRL 3E3A, University of Pennsylvania
E-mail address: shonkwil@math.upenn.edu