Number Theory, hw7

Ethan D. Bolker

December 5, 2013

Here are some exercises that explore number theory in the *Gaussian integers*

$$\mathbb{G} = \{\ a + bi \mid a, b \in \mathbb{Z}\ \}.$$

They're interesting in their own right and will help you review some number theory in $\mathbb{Z}$.

1. Factor 29 and 101 in $\mathbb{G}$.

   Here's a hint you shouldn't need: each of those is a prime congruent to 1(mod 4) in $\mathbb{Z}$, so it's a sum of two squares.

2. Let v and w be the answers to the previous question that lie in the first quadrant (that is, a and b are positive). We know v and w are prime in $\mathbb{G}$, so they are relatively prime. Use the Euclidean algorithm in $\mathbb{G}$ to find Gaussian integers x and y such that
   $$vx + wy = 1.$$

3. (Optional - I don't know the answer since I haven't looked at the question). You can use the Euclidean algorithm in $\mathbb{Z}$ to solve the Diophanine equation
   $$29x + 101y = 1.$$

   Is there any relation between this solution and the one you found in the previous problem?

4. You can do modular arithmetic in $\mathbb{G}$ just the way you do in $\mathbb{Z}$: define
   $$v \equiv w (\text{mod } z) \text{ when } z \text{ divides } v - w.$$

   Then define the ring $\mathbb{G}_z$ just the way we defined $\mathbb{Z}_n$.

   Here's the first question about this new modular arithmetic. Let $z = n+0i \in \mathbb{Z}$. Show that every Gaussian integer is congruent (mod z) to some $c + di$ with $0 \le c, d < n$.

   Hint: you can do this if you think of division as repeated subtraction when you also allow yourself to subtract ni.

   Then $\mathbb{G}_n$ has n^2 elements.

5. (Optional. I can prove this, cleverly but not easily).

   Show that $\mathbb{G}_z$ has norm(z) elements.

   (The previous problem does this when z has zero imaginary part.)

   For example, when $z = 2 + i$, every Gaussian integer is congruent to one of

   $$\{\ 0, i, 1 + i, 2, 2 + i\}$$

   . These are the essentially the points in the square with vertices $0, z, iz, z + iz$.

6. Figure out (and prove) Fermat's Little Theorem for modular arithmetic in the Gaussian integers.

   If you can't see this right away in reasonably abstract terms you can at least compute some examples. What happens with the Gaussian primes 3 and $2+i$?