The universe is not only queerer than we suppose but queerer than we can suppose.
– J.B.S. Haldane

We examine the number of solutions to the equation $x^2 + y^2 = n$ with $x, y \in \mathbb{Z}$. We call $\alpha = x + iy$ the related Gaussian integer. Call two solutions equivalent if you can get from one to the other by adding minus signs and/or flipping $x, y$. For example, $(3, 11)$ and $(11, -3)$ are the same. We actually count the solutions up to equivalence. (While we don’t quite do it, these methods yield the answer for all $n$.)

1. Show (easy!) $(x, y)$ is a solution iff $\alpha \overline{\alpha} = n$. Now write $\alpha \equiv \alpha'$ if either $\alpha \sim \alpha'$ or $\alpha \sim \alpha'$. ($\overline{\alpha}$ denotes the complex conjugate and $\alpha \sim \beta$ means $\beta = u\alpha$, $u$ a unit.) Show that two solutions $(x, y), (x', y')$ are equivalent iff their related $\alpha, \alpha'$ have $\alpha \equiv \alpha'$.

Solution: With $\alpha$ related to $(x, y)$ we have $i\alpha, -\alpha, -i\alpha$ related to $(-y, x), (-x, -y), (y, -x), \overline{x}, -\overline{x}, -i\overline{x}$ to $(y, x), (-x, y), (-y, -x)$.

2. (This problem counts double!) Let $n = p_1 \cdots p_r$ where the $p_i$ are all integer primes and all are of the form $4k + 1$. In $\mathbb{Z}[i]$ write each $p_i = \alpha_i \beta_i$ with $\beta_i = \overline{\alpha_i}$. $\gamma = \gamma_1 \cdots \gamma_r$ with each $\gamma_i \in \{\alpha_i, \beta_i\}$. Note there are $2^r$ choices here.

(a) Setting $\gamma = x + iy$ show that $x^2 + y^2 = n$.
Solution: $\gamma \overline{\gamma} = \prod_i \alpha_i \beta_i = \prod_i p_i = n$.

(b) Show that if $x^2 + y^2 = n$ then there is such a $\gamma = x + iy$.
Solution: Setting $\kappa = x + iy$ we have $\kappa \overline{\kappa} = n$. In $\mathbb{Z}[i]$, $n = \prod_i \alpha_i \overline{\alpha_i}$. By Unique Factorization, $\kappa$ must have precisely one of each $\alpha_i, \overline{\alpha_i}$.

(c) Show that two choices for $\gamma, \gamma'$ give $\gamma \equiv \gamma'$ iff they were either exactly the same choice or exactly the opposite choice.
Solution: By Unique Factorization if $\gamma \sim \gamma'$ they have precisely the same factors. Also, if $\gamma' \sim \overline{\gamma}$ they must have precisely the conjugate factors.

(d) Using the above, find the number of solutions to $x^2 + y^2$.
Solution: The $2^r$ choices split into pairs so there are $2^r - 1$ solutions.
(e) Setting \( n = 5 \cdot 13 \cdot 17 \) use the above to find the four solutions to \( x^2 + y^2 = n \) explicitly.

**Solution:** We factor 
\[
\begin{align*}
n &= (2 + i)(2 - i)(3 + 2i)(3 - 2i)(4 + i)(4 - i)
\end{align*}
\]

We can assume (going to the complex conjugate if needed) \( 2 + i \) is chosen. The four solutions are then
\[
\begin{align*}
(2 + i)(3 + 2i)(4 + i) &= \\
(2 + i)(3 + 2i)(4 - i) &= \\
(2 + i)(3 - 2i)(4 + i) &= \\
(2 + i)(3 - 2i)(4 - i) &=
\end{align*}
\]

3. Let \( n = 2^s \). Describe the factorization of \( n \) in \( \mathbb{Z}[i] \). Argue that the number of solutions to \( x^2 + y^2 = n \) is one.

**Solution:** As \( 2 = (-i)(1 + i)^2 \), \( 2^s \sim (1 + i)^{2s} \) and so we must have \( \gamma = (1_i)^s \). (Once again, 2 is the oddest prime!)

4. Let \( p \) be an integer prime of the form \( 4k+1 \) and let \( n = p^r \). Describe the factorization of \( n \) in \( \mathbb{Z}[i] \). Find the number of solutions to \( x^2 + y^2 = n \). (The cases \( r \) even and \( r \) odd will be slightly different.) Illustrate your results in the case \( n = 3125 = 5^5 \).

**Solution:** Write \( p = \pi \overline{\pi} \) so \( n = \pi^r \overline{\pi}^r \). The possible \( \gamma = \pi^r \overline{\pi}^r - i \) with \( 0 \leq i \leq r \). But \( i, r - i \) give conjugate \( \gamma \). When \( r \) is odd the \( r + 1 \) values of \( i \) become \( (r + 1)/2 \) solutions. When \( r \) is even the value \( i = r/2 \) is by itself and the \( r + 1 \) values become \( \frac{r}{2} + 1 \) solutions. \( 3125 = 5^5 = (2 + i)^5(2 - i)^5 \). The solutions are
\[
\begin{align*}
(2 + i)^5 &= \\
(2 + i)^4(2 - i) &= 5(2 + i)^3 = \\
(2 + i)^3(2 - i)^2 &= 25(2 + i) = 50 + 25i
\end{align*}
\]

5. Let \( p \) be an integer prime of the form \( 4k+3 \) and let \( n = p^r \). Describe the factorization of \( n \) in \( \mathbb{Z}[i] \). Find the essential number of solutions to \( x^2 + y^2 = n \). (The cases \( r \) even and \( r \) odd will be slightly different.)

**Solution:** As \( p \) is a Gaussian prime, \( n = p^r \) is the factorization in \( \mathbb{Z}[i] \). When \( r \) is odd there is no \( \gamma \), so no solution; when \( r \) is even there is one solution, \( \gamma = p^{r/2} \). That is, \( x = p^{r/2}, y = 0 \).
6. (Just for Fun) Presidential Trivia:

(a) Which president had a great stamp collection?
Solution: Franklin Delano Roosevelt. He had the State Department forward him interesting stamps.

(b) Which was the fattest president?
Solution: Taft. Yes, surprisingly, he was an excellent dancer.

(c) Which two presidents died on the same day?
Solution: John Adams and Thomas Jefferson, precisely on the 50th anniversary of the signing of the Declaration of Independence.

(d) Which presidents were divorced?
Solution: Ronald Reagan and Donald Trump

7. Describe all pairs \( a \in \mathbb{Z}, n \geq 2 \) such that Eisenstein’s Criterion implies that \( x^n - a \) is irreducible.
Solution: \( n \) is immaterial. \( a \) must have some prime factor that is only to the first power. (BTW, other values do give irreducible polynomials, we just don’t derive their irreducibility from Eisenstein.)

Nothing is more fruitful - all mathematicians know it - than those obscure analogies, those disturbing reflections of one theory in another; those furtive caresses, those inexplicable discords; nothing also gives more pleasure to the researcher. The day comes when the illusion dissolves; the yoked theories reveal their common source before disappearing. As the Gita teaches, one achieves knowledge and indifference at the same time.

André Weil
(Note: “indifference” is a controversial translation of the original Sanskrit, “detachment” is often used instead)