Berkeley Mathematics Circle

Richard Borcherds

May 7, 2013

1. Recall Pythagoras's theorem $a^2 + b^2 = c^2$ for the sides of a right-angles triangle. When can a, b, c be integers? Everyone knows the case $3^2+4^2 = 5^2$. Other solutions include $5^2 + 12^2 = 13^2$, $7^2 + 24^2 = 25^2$, ... The problem is to describe all solutions. We take out any common factors, so can assume that c is positive and coprime to a and b to eliminate trivial variations.

2. Algebraic solution: c must be odd (why?) so exactly one of a, b is odd: we may as well assume a is odd and b is even. Then $(b/2)^2 = ((c-a)/2)((c+a)/2)$, so the two factors on the right are both squares as they are coprime and their product is a square. So $c - a = 2s^2$, $c + a = 2t^2$ for some s, t. This gives the solution $c = s^2 + t^2$, $a = t^2 - s^2$, $b = 2st$, for $s < t$ positive integers with one odd, one even.

3. What are s and t for the solutions in part 1? What solution do you get from $s = 2$, $t = 5$?

4. Geometric solution: Put $x = a/c$, $y = b/c$, so x and y are rational with $x^2 + y^2 = 1$. In other words we want to find rational points on the unit circle. We can do this by drawing the line through $(-1, 0)$ and (x, y) : it intersects the y-axis in a point $(0, t)$. Note that t is rational or infinity if and only if both x and y are rational. Formulas: $t = y/(x + 1)$, $x = (1 - t^2)/(1 + t^2)$, $y = 2t/(1 + t^2)$.

5. Find the values of t corresponding to the 8 solutions $(\pm 3)^2 + (\pm 4^2) = 5^2$, $(\pm 4)^2 + (\pm 3^2) = 5^2$. Find the right angled triangles with integer sides corresponding to t an integer.

6. So we have two pictures of solutions: we can think of them either as points in a rational line plus infinity, or as rational points on a unit circle. (In algebraic geometry the circle and line are said to be "birational".)

7. The solutions form a GROUP. Reason: points on the unit circle correspond to rotations, and we can multiply rotations. Formulas: $x = \cos\theta, y = \sin\theta$. $\sin(\theta_1 + \theta_2) = \sin(\theta_1)\cos(\theta_2) + \cos(\theta_1)\sin(\theta_2)$, $\cos(\theta_1 + \theta_2) = \cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2)$. So $(x_1, y_1)(x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$.

8. What solution do we get by multiplying the solution $3^2+4^2 = 5^2$ by itself? What happens if we multiply it by $4^2 + 3^2 = 5^2$?

9. We have $t = \tan(\theta/2)$. This is a useful substitution for doing integrals of rational functions of $\sin\theta$ and $\cos\theta$, because $\sin\theta = 2t/(1+t^2)$, $\cos\theta = (1-t^2)/(1+t^2)$, and $d\theta = 2dt/(1+t^2)$. The geometric meaning of this is that we are turning an integral over the unit circle into an integral over the y-axis by projecting from the point $(-1, 0)$. Example: use this to find the integral $\int_0^\theta d\theta/(2+\cos\theta)$.

10. These formulas are not so easy to remember. Better to put $(x, y) = x + iy$ with $i^2 = -1$: then we are just multiplying complex numbers of absolute value 1.

11. Recall geometric meaning of operations on complex numbers: Addition is addition of vectors, multiplication multiples lengths and adds angles, absolute value $\sqrt{z\overline{z}}$ is distance from 0 and has the usual properties $|z_1 z_2| = |z_1| \times |z_2|$, $|z_1 - z_2| \leq |z_1| + |z_2|$ ("metric inequality").

12. Suppose m and n are both sums of two squares. Show that mn is a sum of two squares. (Write m and n as the squares of the absolute values of Gaussian integers, then multiply these Gaussian integers. This gives the identity $(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2$. There are similar identities for sums of 4 and 8 squares that you can get by replacing the complex numbers by quaternions of octonions.)

13. Write 5, 13, 17 as a sum of two squares, and use this to find right angled triangles of sides 5, 13, 17. There are 8 ways of writing 5 as a sum of 2 squares, corresponding to the 8 ways a knight can move in chess.

14. Which primes are sums of two squares? $5, 13, 17, 29, 37$ are, $3, 7, 11, 19, 23, 31$ are not. What is the pattern?

15. Any square has remainder 0 or 1 mod 4. Show that numbers that are 3 mod 4 cannot be a sum of two squares. Find a positive number 1 mod 4 that is not a sum of two squares.

16. Show that any number 7 mod 8 cannot be a sum of 3 squares. Slightly trickier: show that a number of the form $4^m(8n+7)$ cannot be a sum of 3 squares. (Conversely any positive integer not of this form is a sum of 3 squares, but this is much harder to prove.)

17. Find an example to show that if m and n are sums of 3 squares, then mn need not be a sum of 3 squares.

18. Are all primes 1 mod 4 a sum of 2 squares? Yes, but this is not so easy to show. There are two easy implications: (1) if p is a prime that is a sum of 2 squares then $x^2 + 1$ is divisible by p for some x, and (2) If $x^2 + 1$ is divisible by p for some x then p is 1 mod 4. We will show both these implications "reverse".

19. Suppose p is 1 mod 4. Then Z/pZ^* is cyclic of order $p-1$, which is divisible by 4. The element -1 has order 2 in this group. Pick any generator g: then $g^{(p-1)/4}$ has square -1 (why?).

20. This gives an efficient algorithm for finding a square root of -1 mod p. Just pick any generator and raise it to the power of $(p-1)/4$. Problem: how do we find a generator? Answer: random guessing. For any random element g, there is a 1 in 2 chance that $g^{(p-1)/4}$ has square -1. Example: if $p = 17$ we first try $g = 2$ which does not work, then try $g = 3$ which does.

21. How do we find $g^{(p-1)/4}$ is p is very large, say 1000 digits (on a computer of course)? We first work out g^1, g^2, g^4, and so on mod p by repeated squaring. Key point: since we reduce mod p every time we never need to use more than 2000 digits. Then we work out g^k by writing k in binary: for example $g^{37} = g^1 \times g^4 \times g^{32}$. (Rather surprisingly this is not always the most efficient way to work out g^k. This method takes 6 multiplications to work out g^{15}; show how to work out g^{15} using only 5 multiplications.)

22. Suppose we have found a solution of $z^2+1 = np$. How do we find a solution of $x^2 + y^2 = p$? Write these in terms of Gaussian integers: $(z+i)(z-i) = np$, $(x+iy)(x-iy) = p$. So the highest common factor of $z+i$ and p should be $x \pm iy$) times a unit i^k. How do we find this highest common factor for Gaussian integers? Same way as for integers: use Euclid's algorithm.

23. Recall Euclid's algorithm for finding the greatest common divisor of two positive integers: repeatedly replace the largest one by the remainder when dividing by the other. Use this to find the greatest common divisor of 39 amd 15. (For small numbers it is often faster just to factorize the numbers, but for large numbers with hundreds of digits it is far faster to use Euclid's algorithm.)

24. Key point: we can do division with remainder for Gaussian integers: Given a, $b \neq 0$ we can find q, r with $a = bq + r$, $|r| < |b|$. This is because we can find q with $|q - a/b| < 1$: the plane is covered by unit disks with centers the lattice points q. Example: find the greatest common divisor of $5 + i$ and 13: $13/(5+i) = (65-5i)/26$ which is closest to the Gaussian integer 2, so put $13 = 2(5+i)+3-2i$. The remainder is $3-2i$, so now we divide $(5+i)/(3-2i) = 1+i$ with no remainder. So the greatest common divisor of 13 and $5 + i$ is $3 - 2i$. This gives the expression of 13 as the sum of 2 squares $13 = 3^2 + 2^2$.

25. Of course this is a silly way to write 13 as the sum of 2 squares: it is easier to find the solution by trial and error. However for large numbers this method is MUCH faster than trial and error. Suppose a computer can do a billion operations a second. Estimate very roughly how long it will take to write a hundred digit prime as a sum of 2 squares using trial and error, and using the method above.

26. How many ways can we write a number as a sum of 2 squares? $5^0, 5^1, 5^2$ can be written as a sum of 2 squares in 4, 8, 12 ways. Guess how many ways 5^3 can be written as a sum of 2 squares. In general we have $5^n = z\overline{z}$ where $z = i^k(2+i)^m(2-i)^{n-m}$ and $\overline{z}$ is the complex conjugate of z. There are 4 possibilities for k and $n+1$ possibilities for m, so this gives $4(n+1)$ ways to write $5^n = x^2 + y^2$ as a sum of 2 squares where $z = x + iy$.