Feedback

The Editor apologies to Lienhard Wimmer for the fact that the beginning of his Feedback item on page 532 in the November 2016 issue of the *Gazette* was missing. Here is the corrected Feedback.

On 'Remembering Spherical Geometry': Lienhard Wimmer writes: The authors of [1] describe a number δ that is related to the area of the spherical triangle by an equation called *Lexell's equation*. In fact this number has its own geometrical meaning and it is neither unknown nor nameless.

Let ABC be a triangle on the unit sphere centred at O. This number is six times the volume of the tetrahedron $OABC$. It has at least two names. In [2] it is called the *norm* of a triangle, whereas in German literature it is also known as the *Eckensinus* [sine of a (spatial) vertex] – this name is due to Karl von Staudt as reported in the excellent book [3]. The same number is also known as the *solid angle of the spherical triangle*. As literature please consult [4].

Of course the number is not an intrinsic number of spherical geometry but is a property of the embedding Euclidean space. Nevertheless many theorems of plane Euclidean geometry that depend on the area of a triangle have two counterparts. For example the area of a plane triangle is given by

$$A = \tfrac{1}{2}ab \sin\gamma.$$

The norm δ of the spherical triangle is then

$$\delta = \sin a \sin b \sin\gamma,$$

where the spherical area ε is given by the useful but litte known formula

$$\tan\frac{\varepsilon}{2} = \frac{\sin\gamma}{\cot\frac{a}{2}\cot\frac{b}{2} + \cos\gamma}.$$

A second example is the locus of a point C such that the area of the triangle ABC, for two fixed points A and B, remains unchanged. In plane geometry this locus is a line parallel to the line through A and B. In spherical geometry there are two possible loci. If we use the norm of a triangle and if the great circle through A and B is the equator, the locus is a circle of latitude. If we use the spherical area, this locus is the circle of Lexell given by C and the antipodal points A^c and B^c.

References

1. John Conway and Alex Ryba, Remembering Spherical Geometry, *Math. Gaz.* 100 (March 2016) pp. 1-8.
2. Murray Klamkin, *Mathematics Magazine 46* (1973), pp. 208-211.
3. Rudolf Sigl, *Ebene und Sphärische Trigonometrie*, Herbert Wichmann Verlag, Karlsruhe (1977).
4. Folke Eriksson, On the Measure of Solid Angles *Mathematics Magazine* **63** (3), (1990) pp. 184-187.

https://doi.org/10.1017/mag.2017.25 Published online by Cambridge University Press

On 'Cyclotomy and the heptadecagon' Peter Shiu writes: In [1], I stated that: 'With hindsight, the construction of the regular heptadecagon can be accomplished with only a minimal amount of the theory [of cyclotomy]', and 'Whereas it is easy to exponentiate in modular arithmetic, the computation of the discrete logarithm is difficult'. The following items are clarification supplements to these two statements.

(1) Let $\alpha = \dfrac{2\pi}{17}$, and set

$$a = \cos\alpha + \cos 4\alpha, \qquad b = \cos 2\alpha + \cos 8\alpha, \qquad e = a + b,$$
$$c = \cos 3\alpha + \cos 5\alpha, \qquad d = \cos 6\alpha + \cos 7\alpha, \qquad f = c + d,$$

so that $a > b$, $c > d$ and $e > f$. Making use of

$$1 + \cos\alpha + \cos 2\alpha + \ldots + \cos 16\alpha = 0$$

and the trigonometric identity $\cos(A + B) + \cos(A - B) = 2\cos A \cos B$, we find that $2(e + f)$, ef, $4ab$ are all equal to -1. It follows that e, f are solutions to the quadratic $x^2 + \frac{1}{2}x - 1 = 0$, and that a, b are solutions to $x^2 - ex - \frac{1}{4} = 0$, so that $4\{e,f\} = -1 \pm \sqrt{17}$ and $2\{a,b\} = e \pm \sqrt{e^2+1}$. Therefore $8\{a, b\} = -1 + \sqrt{17} \pm \sqrt{34 - 2\sqrt{17}}$, and similarly $8\{c,d\} = -1 - \sqrt{17} \pm \sqrt{34 + 2\sqrt{17}}$. We also deduce from $\cos\alpha + \cos 4\alpha = a$ and $2\cos\alpha\cos 4\alpha = c$ that $\cos\alpha$ is the larger of the two solutions to $x^2 - ax + \frac{1}{2}c = 0$, so that

$$2\cos\alpha = a + \sqrt{a^2 - 2c} = a + \sqrt{1 + \tfrac{1}{2}b - c},$$

and hence

$$16\cos\alpha = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

Therefore the angle $\alpha = \dfrac{2\pi}{17}$ can be constructed by Euclidean means. However, it will be grossly misleading to say that the theory of cyclotomy has nothing to do with this solution.

(2) With a computing machine, it is easy to find primes of modest size, and not difficult to find large ones; for our purpose, modest size means about 10^{16}, and large means exceeding 10^{200}, say. Indeed, by trial division, it is easy to verify that

$$p = 10^{16} - 63 = 9\,99999\,99999\,99937$$

is a prime. Next, let q be such that $q - 1 = FR$, where the complete factorisation of F is known. If $F > R$ then there is a simple procedure, based on Pocklington's theorem (see, for example, [2, Theorem 4.1.3]), which establishes whether q is a prime or not. Thus, setting

$$F = 2 \times 3 \times 7 \times 11 \times 13 \times 17\left(10^{16} - 63\right)^6, \qquad R = 10^{100} - 21,$$

so that $F > R$, the procedure can be used to verify that $q = FR + 1$ is a large prime. The numbers 63 and 21 in the above are chosen so that 5 is a

https://doi.org/10.1017/mag.2017.25 Published online by Cambridge University Press

primitive root modulo p and modulo q, and the discrete logarithms of a given t, with respect to this primitive root, are then the solutions x and y to the congruences $5^x \equiv t \pmod{p}$ and $5^y \equiv t \pmod{q}$. For concreteness, we take

$$t = \frac{10^{16} - 1}{3} = 3\,33333\,33333\,33333.$$

The computation of x cannot be described as easy—the brute-force method of searching through $x = 0, 1, 2, \ldots$ successively is not practical, because the answer may not emerge before the cows-come-home! A bit of theory and a fair amount of computing time are necessary. Anyway, on the implementation of Pollard's rho method (see, for example, [2, Section 5.2.2]), after some 12 minutes spent on about 10^8 iterations, each involving several multiplications modulo p and modulo $p - 1$, our Python program delivers the answer

$$x = 7\,80218\,65857\,44146.$$

That x is indeed the sought after discrete logarithm can be verified easily, because exponentiation modulo p can be done by the 'square-and-conquer' method. More specifically, the residue classes $5^{2^i} \pmod{p}$ can be obtained by repeated squaring, so that the class $5^x \pmod{p}$ can be delivered from the binary representation of $x = \sum \varepsilon_i 2^i$, where $\varepsilon_i = 0, 1$ for $i \geqslant 0$. Thus from

$$x = \big(110\,11101\,11000\,00001\,10000\,01111\,11110\,10100\,01000\,11000\,10010\big)_2,$$

verification involves fewer than 100 multiplications (mod p), and the time taken is only a tiny fraction of a second.

With the current knowledge of the discrete logarithm problem, the task of computing y is more than challenging, even on a supercomputer. On the other hand, if y is known, given, or chosen, then $5^y \pmod{q}$ can be delivered by the square-and-conquer method, in a fraction of a second on a small machine. Thus, exponentiation modulo a prime is a 'one-way function'.

References

1. Peter Shiu, Cyclotomy and the heptadecagon, *Math. Gaz.* **100** (July 2016) pp. 288–297.
2. Richard Crandall and Carl Pomerance, *Prime Numbers: A Computational Perspective* (2nd edn.) Springer (2005).

On Note 100.28; Sergiy Koshkin writes: After the note *Mixing Angle Trisection with Pythagorean Triples* was published it came to the author's attention that the problem of finding all integer self-trisecting triangles was solved by Alexander Oppenheim back in 1954 (as reported by R. Guy, [1]) using number theoretic methods, with the method generalised to self-multisecting and more general triangles in 1967, [2].

1. R. Guy, Triangles with $B = 3A$, $2B = 3A$, *Bulletin of the Malayan Mathematical Society*, **1** (1954) pp. 56-60.

https://doi.org/10.1017/mag.2017.25 Published online by Cambridge University Press

2. D. Daykin, A. Oppenheim, Classroom Notes: Triangles with Rational Sides and Angle Ratios, *Amer. Math. Monthly*, **74**(1) (1967) pp. 45-47.

On Note 100.35: Paul Stephenson writes: The result shown by this pretty proof without words is equivalent to the relation $Tet_n + Tet_{n-1} = Pyr_n$, where Tet_n is the nth tetrahedral number, $\frac{1}{6}n(n+1)(n+2)$, Pyr_n the nth pyramidal number, $\frac{1}{6}n(n+1)(2n+1)$. This is the three-dimensional analogue of the relation $T_n + T_{n-1} = S_n$, where T_n is the nth triangle number, $\frac{1}{2}n(n+1)$, S_n the nth square, n^2. The latter represents a horizontal slice through the respective tetrahedra standing side-by-side. We can in turn write: $Pyr_n + Pyr_{n-1} = Oct_n$, where Oct_n is the nth octahedral number, $\frac{1}{3}n(2n^2+1)$. The pyramids fit base-to-base. For these and other interrelations between the figurate numbers which might interest readers who give workshops for young people, see [1].

Reference

1. Paul Stephenson, www.magicmathworks.org/masterclasses, then 'Numbershapes – figurate numbers', then 'Number shapes session notes (pdf)'.

10.1017/mag.2017.25

In the pipeline for July 2017

Stan Dolan	Lyness cycles
Martin Josefsson	Generalisation of a quadrilateral duality theorem
	Properties of bisect-diagonal quadrilaterals
David Treeby	Finding sums of powers using physical arguments
G. J. O. Jameson	Expressing harmonic sums as fractions
Jeehoon Kang	Brilliance or Steadiness?
Jonathan Hoseana	An Exotic Technique of Integration Based on the Parametrisation of Conics
Seán M. Stewart	Some alternative derivations of Craig's formula
Christopher D. Hollings	R. S. Ball's *Mechanics*: bringing Newton to the masses?

https://doi.org/10.1017/mag.2017.25 Published online by Cambridge University Press