ADDITIONAL NOTES

Chapter I

1 ♠I:1 (page 29) The 10^{300} result is due to Brent, Cohen and te Riele in *Math. Comp.* 57 (1991) 857–868. 'eight distinct prime factors' is due to Hagis in *Math. Comp.* 35 (1980) 1027–1032. We also know that any odd perfect number must have at least 47 prime factors (not necessarily distinct), see Hare in *Math. Comp.* 74 (2005), 1003–1008. The fact that the largest prime factor exceeds 10^8 is due to Goto and Ohno in http://www.ma.noda.tus.ac.jp/u/tg/perfect/perfect.pdf.

2 ♠I:2 (page 30)

♠Added June 2009♠

Despite the "near miss' character of Chen's theorem, it is a key ingredient in Ford's proof of the Sierpiński conjecture: see note ♠E:1.

Chapter II

1 ♠II:1 (page 48) Choi's construction was used by Chen (*Proc. American Math. Soc.* 128 (2000), 1613–6) to show that a non-zero proportion (more technically, a positive asymptotic density) of the odd numbers are *not* of the form $2^n \pm p^\alpha q^\beta$, where n, α and β are non-negative integers and p and q distinct primes. Again using Choi's construction, Chen also showed (*J. Number Theory* 98 (2003), 310–319) that, for any positive odd r, there is an infinite arithmetic progression of k such that $k^r - 2^n$ has at least two distinct prime factors for all positive integers n. Dirichlet's theorem then shows that there are infinitely many *prime* k with this property.

Chapter III

1 ♠III:1 (page 66) Burgess showed that the least non-residue (mod p) was of order roughly $p^{1/4\sqrt{e}}$. Hildebrand (*Michigan Math. J.*, 34 (1987), 57–62) showed that the same was true for the least pair of consecutive non-residues.

Chapter VII

1 ♠VII:1 (page 162) Mordell proved that, for fixed k, there are only finitely many integer points on such a curve, in other words that the difference between y^2 and x^3 tends to infinity (unless $x^3 = y^2$, $k = 0$ and the curve is singular). "How fast?" is an interesting question. Marshall Hall suggested in 1971 that it grew proportionally to $\sqrt{x}$, but Elkies

has recently discovered (5853886516781223, 447884928428402042307918) as an integral point on $y^2 = x^3 + 1641843$, which has $|y^2 - x^3|/\sqrt{x} \approx 0.0215$, which makes it more likely that it grows "almost proportionally" to $\sqrt{x}$. Elkies' work is at http://www.math.harvard.edu/~elkies/hall.html, and 'Rational Points Near Curves and Small Nonzero $|x^3 - y^2|$ via Lattice Reduction', Proc. ANTS-IV (ed. W. Bosma), Springer Lecture Notes in Computer Science 1838, Springer-Verlag, 2000, 33–64. We should note the gulf between these estimates and those from (28) and its improvements, which are of the form $c\sqrt{\log x}$ for very small c.

2 ♠VII:2 (page 162) While the Weierstrass form (13) is the most general form over the integers (if we are working modulo 2, we need to allow for an xy term as well), neither it nor (15) is the most efficient for computation, a requirement of many modern uses (see VIII). This is generally thought to be the inverted formulation of the Edwards curve

$$x^2 + y^2 = a^2 + a^2x^2y^2,$$

where $a = \frac{1}{2}$ corresponds to the special case of a circle. Addition of (x_1, y_1) and (x_2, y_2) is defined as

$$\begin{cases} x_3 = \dfrac{1}{a}\dfrac{x_1y_2 + x_2y_1}{1 + x_1y_1x_2y_2} \\ y_3 = \dfrac{1}{a}\dfrac{y_1y_2 - x_1x_2}{1 - x_1y_1x_2y_2} \end{cases},$$

which means we do not need a separate formula for doubling, unlike the Weierstrass form's (17″) versus (17′). In this formulation $(x = 0, y = a)$ is the zero point of the addition law, $(0, a)$ is a point of order two, and $(\pm a, 0)$ are points of order four. Every curve with a point of order four is equivalent to an Edwards curve. See Edwards in Bull. A.M.S. 44 (2007) 393–422. The inverted formulation is discussed by Bernstein and Lange (Proc. AAECC 2007 (eds. Boztas,S. & Lu,H.-F.), Springer Lecture Notes in Computer Science 4851, Springer, Berlin-Heidelberg-New York, 2007, pp. 20–27). The various addition formulae, and the operation counts, can be found at http://www.hyperelliptic.org/EFD.

♠Added May 2009; updated June 2009♠

Diagrams of the Edwards curve, showing the addition laws, can be found as Figure 1 in the paper 'Faster Pairing Computation' by Arène *et al.* available from http://arxiv.org/abs/0904.0854, though the paper as a whole is much deeper than we have ventured.

3 ♠VII:3 (page 162) Fermigier's work is on his Web page
http://www.math.jussieu.fr/~fermigie/dvi/rang22.dvi
and *Acta Arith.* 82 (1997) 359–363. The example with 22 independent points has

$$A = -940299517776391362903023121165864,$$

$$B = 10707363070719743033425295515449274534651125011362.$$

R. Martin and W. McMillen (unpublished) have found examples with 23 and 24 independent points: see K. Rubin and A. Silverberg in *Bull. American Math. Soc. (N.S.)* 39 (2002) 455–474.

4 ♠VII:4 (page 163) Geometers define the complexity of an algebraic curve by means of the *genus* — see, for example, Fulton, *Algebraic Curves, An Introduction to Algebraic Geometry* (W.A. Benjamin Inc, 1969) for a precise definition. A conic section, i.e. a quadratic in x and y, has genus zero. A *non-singular* elliptic curve has genus one, whereas a singular one can be reduced to a conic, e.g. $y^2 = x^3 + 2x^2 + x$ can be written

as $\left(\frac{y}{x+1}\right)^2 = x$, or $Y^2 = x$, which is a conic. A typical curve of higher genus might be $y^2 = x^5 + 1$.

5 ♠VII:5 (page 163) A.-S. Elsenhans and J. Jahnel searched for small (< 1000) sums of three cubes with $|x|, |y|, |z| \le 10^{14}$, and found examples such as

$$\begin{aligned} 52 &= 60702901317^3 + 23961292454^3 - 61922712865^3 \\ &= 1232911859663^3 + 343101441461^3 - 1241705896626^3. \end{aligned}$$

They also found

$$24 = 15584139827^3 - 2901096694^3 - 15550555555^3,$$

and several representations for 81, which seems to imply that there is a peculiar difficulty with 3. See http://www.uni-math.gwdg.de/tschinkel/gauss/Elkies.pdf.

6 ♠VII:6 (page 163) The Ren and Tsang paper shows that the number of numbers less than N which are *not* so representable is essentially less than $N^{17/18}$, i.e. "almost all" numbers are so representable, and indeed even with three of the numbers being primes. The precise definition of 'is essentially less than' would take too much terminology.

7 ♠VII:7 (page 164) The true Hadju–Herendi formula for solutions of $y^2 = x^3 + ax + b$, with discriminant Δ, is

$$|x|, |y| \le \exp(5 \cdot 10^{64} c_1 \log(c_1)(c_1 + \log(c_2))),$$

where

$$c_1 = \frac{32 + \sqrt{\Delta}(8 + \frac{1}{2}\log(\Delta))^4}{3}, \qquad c_2 = 10^4 \max(16a^2, 256\Delta^{2/3}).$$

Chapter VIII

1 ♠VIII:1 (page 203)

♠Added January 2010♠

On December 12, 2009, a large team factored the 768-bit (232 digit) number once issued as an RSA challenge. The details are in http://eprint.iacr.org/2010/006.pdf. This beats the previous record for 'general' numbers: a 200-digit number set in May 2005 (http://www.loria.fr/~zimmerma/records/rsa200). The factorization of numbers of a special form has also moved on, and the corresponding record is the Mersenne number $2^{1039} - 1$, announced by Aoki *et al.* in Proc. ASIACRYPT 2007, Springer Lecture Notes in Computer Science 4833, pp. 1–12.

Chapter VIII

1 ♠VIII:1 (page 204) The observation about the number of factors is from Granville's review: *Math. Reviews* 93m:11137. This discrepancy is important since it appears to explain why Carmichael numbers are not found as often as "we think they ought to be"—see A. Granville and C. Pomerance 'Two contradictory conjectures concerning Carmichael numbers' in *Math. Comp.* 71 (2002) 883–908.

2 ♠VIII:2 (page 206) The `https` protocol itself is described in Internet RFC 2818. This uses the Transport Layer Security, whose latest definition is in Internet RFC 4346, which uses Diffie–Hellman in a very similar way to (12). The web server B sends its x^b, as well as x and p, as part of the start-up process. The client A can choose a compute x^a and x^{ab}, use x^{ab} to encrypt its data, and send x^a to B, which can compute x^{ab} to decrypt the data, and encrypt its own. The Internet documents are

at ftp://ftp.rfc-editor.org/in-notes/rfc2818.txt and ftp://ftp.rfc-editor.org/in-notes/rfc4346.txt.

3 ♠VIII:3 (page 206) A variant on the Diffie–Hellman scheme, which uses finite fields of size $N = 2^n$ rather than of prime size, and which therefore seems much more adapted to binary computation, can be cracked in time proportional to $M(n)^c = \exp(c \log^{1/3} N (\log\log N)^{2/3})$—see Coppersmith's paper 'Fast evaluation of logarithms in fields of characteristic two', *IEEE Trans. Inform. Theory* IT–30 (1984) 587–594.

4 ♠VIII:4 (page 207) The first proof that knowing x and *any* x'' was polynomial-time equivalent to factoring N was due to May 'Computing the RSA secret key is deterministic polynomial time equivalent to factoring' in *Proc. CRYPTO 2004* (Springer Lecture Notes in Computer Science 3152, Springer-Verlag, Berlin–Heidelberg–New York, 2004), 213–219. An improved version by Coron and May is 'Deterministic Polynomial-Time Equivalence of Computing the RSA Secret Key and Factoring' in *J. Cryptology* 20 (2007) 39–50. While polynomial-time, the complexity of these has not been analysed in detail, and it is likely to be very expensive in practice. These equivalences use Coppersmith's method described in the next paragraph.

5 ♠VIII:5 (page 207) One attack on RSA using Coppersmith's method is described by Crouch and Davenport in *Proc. 8th. IMA Conf. Cryptography and Coding* (Springer Lecture Notes in Computer Science 2260, ed. B. Honary, Springer-Verlag, Berlin–Heidelberg–New York, 2001) 329–338.

♠Added June 2013♠

A good description of why RSA encryption in practice needs more precautions than we have given here is given by Boneh, Joux and Nguyen in"Why textbook ElGamal and RSA encryption are insecure" in *Advances in Cryptology — ASIACRYPT 2000* (Springer Lecture Notes in Computer Science 1976, ed. T. Okamoto, Springer-Verlag, Berlin–Heidelberg–New York, 2000) 30–43.

6 ♠VIII:6 (page 207) Sophie Germain proved that, if $x^5 + y^5 = z^5$ is soluble, then one of x, y and z is divisible by 5, and more generally if 5 is replaced by any 'Sophie Germain' prime

7 ♠VIII:7 (page 207) Bernstein has also proved that checking that n is not a perfect power is very cheap, in fact roughly $\log n$.

Exercises

1 ♠E:1 (page 212) The verification of Carmichael's conjecture up to $10^{10^{10}}$ is due to Ford in 'The distribution of totients', *Ramanujan J.* 2 (1998), 67–151. Sierpiński's conjecture, that every $k > 1$ *is* some multiplicity of $\phi(n)$, i.e. that there is some m such that $\phi(n) = m$ has precisely k solutions, has recently been proved by Ford in *Ann. of Math.* (2) 150 (1999) 283–311. The proof makes essential use of Chen's theorem, page 30.