value of a we use the relation $10a \equiv -1 \pmod{p}$ to write $10a + 1 = pk$ for some integer k. Considering the inequality $0 < a < p$, we obtain the validity of $\frac{1}{p} < k < 10 + \frac{1}{p}$ for any prime p other than 2 or 5. This fact, together with $k \neq 10$, implies that $0 < k < 10$. Thus we have $pk \equiv 1 \pmod{10}$ with $0 < k < 10$. Now, if $u = 1$ then the conditions $pk \equiv 1 \pmod{10}$ and $0 < k < 10$ imply that $k = 1$, and consequently $a = \frac{p-1}{10}$. A similar argument implies (1) for the other values of u.

This completes the proof.

Acknowledgement: I express my gratitude to Professor Underwood Dudley for careful reading of the manuscript and giving many valuable suggestions and corrections, which improved the presentation of the Note.

10.1017/mag.2019.112

MEHDI HASSANI

Department of Mathematics, University of Zanjan, University Blvd., 45371-38791, Zanjan, Iran

e-mail: *mehdi.hassani@znu.ac.ir*

103.31 Factorising numbers with oracles

A useful classroom game

A teacher asks the students to determine the values of two positive integers a, b from the given values of the product ab, and the sum $a + b$. The students try to factorise the product, and see if the sum of the factors is the same as that for the given sum. If we set a, b to be primes of modest size, the game becomes more of a challenge, because factorisation is no longer easy.

The aim of the exercise is, of course, the introduction of the quadratic equation. The identity $(x - a)(x - b) = x^2 - (a + b)x + ab$ reveals that the game amounts to finding the roots of the equation obtained by setting the right-hand side to be zero. There is now a good incentive for the derivation of the formula for the solutions of a quadratic equation, and the game is over with the values for a, b being given by

$$a, b = \frac{(a + b) \pm \sqrt{(a + b)^2 - 4ab}}{2}. \tag{1}$$

However, a well-informed teacher may remind the students of the salient point concerning the game:

> *The factors of a product can be recovered from the values of the product and the sum of the factors, without resorting to a brute force factorisation scheme.*

A generalisation

Generalising the game we let

$$N = p_1 p_2 \dots p_k, \tag{2}$$

where $p_1, p_2, \dots, p_k$ are distinct primes; we suppose that the value of N is given, but not any of the primes p_h. Consider the accompanying polynomial

$$f(x) = (x - p_1)(x - p_2)\dots(x - p_k) = x^k - e_1 x^{k-1} + e_2 x^{k-2} - \dots + (-1)^k e_k \tag{3}$$

where e_h is the h th elementary symmetric polynomial of $p_1, p_2, \dots, p_k$, that is

$$e_h = \sum_{1 \leqslant j_1 < j_2 < \dots < j_h \leqslant k} p_{j_1} p_{j_2} \dots p_{j_k}, \qquad h = 1, 2, \dots, k; \tag{4}$$

in particular, $e_k = N$ is known. If we are supplied with the values for all the other coefficients e_h, then we can recover the individual values of the primes p_h. More specifically, for any input x, we can now compute $f(x)$, so that the interval bisection method for the evaluation of the roots of $f(x) = 0$ can be used to deliver p_h.

Using Horner's method to evaluate an individual $f(x)$, the number of multiplications involved is only k, and $2^k < N$. The number of bisections required for a single root p_h is of order $\log N$, so that the complete factorisation of N can be done 'efficiently', in the sense that the total number of basic arithmetic operations involved is bounded by a fixed power of $\log N$; in common parlance, the procedure is 'polynomial-time in $\log N$'. We remark, *en passant*, that a similar process for the determination of whether a number is a perfect power of an integer is also efficient.

The arithmetic functions $\phi(n)$ and $\sigma(n)$

Euler's totient function $\phi(n)$ counts the numbers k in $1 \leqslant k \leqslant n$ which are coprime with n; it is a multiplicative arithmetic function in the sense that $\phi(mn) = \phi(m)\phi(n)$ when m, n are coprime. The arithmetic function $\sigma(n)$ is the sum of the divisors of n, and it is also multiplicative. It then follows from (2) that

$$\phi(N) = (p_1 - 1)(p_2 - 1)\dots(p_k - 1), \sigma(N) = (p_1 + 1)(p_2 + 1)\dots(p_k + 1), \tag{5}$$

so that, by (3),

$$\phi(N) = (-1)^k f(1), \qquad \sigma(N) = (-1)^k f(-1).$$

In general, the factorisation of a large number N is difficult, and indeed so is the determination of the values for either $\phi(N)$ or $\sigma(N)$. If we know the prime factorisation of N, then $\phi(N)$ and $\sigma(N)$ can be computed from their respective formulae; at least in this sense, one suspects that the factorisation of N is 'more difficult' than the determination of $\phi(N)$ and $\sigma(N)$. There is now the interesting problem of considering the converse:

> *Can the values of $\phi(N)$ and $\sigma(N)$ be used to deliver the factorisation of N efficiently*?

https://doi.org/10.1017/mag.2019.113 Published online by Cambridge University Press

The Φ-oracle and the Σ-oracle.

By an *oracle*, we mean a 'black box' that will deliver answers to specific questions involving computations; it will deliver only the sought-after answer, and not the procedure on how it is found. The notion of an oracle was first introduced by Alan Turing in his PhD thesis, and it is now a useful abstract concept in the study of computability and complexity theory.

Suppose then that there is a Φ-oracle which, from any input N, will deliver the value of $\phi(N)$; similarly a Σ-oracle will deliver the value of $\sigma(N)$. Our factorisation problem then amounts to:

> *Armed with such oracles, can we devise an efficient scheme to factorise N ?*

For $k = 2$ in (2), we have $e_1 = p_1 + p_2$, and we already know that N can be factorised with the use of either the Φ-oracle, or the Σ-oracle. Indeed, by (1), we have

$$p_1, p_2 = \frac{e_1 \pm \sqrt{e_1^2 - 4N}}{2}, \text{ where } e_1 = N - \phi(N) + 1, \text{ or } e_1 = \sigma(N) - N - 1; \quad (6)$$

the two formulae for e_1 follow from

$$\phi(N) = f(1) = 1 - (p + q) + pq = 1 - e_1 + N,$$
$$\sigma(N) = f(-1) = 1 + (p + q) + N = 1 + e_1 + N.$$

For $k = 3$, the polynomial $f(x)$ in (3) is a cubic with coefficients e_1, e_2 satisfying

$$\phi(N) = -f(1) = -1 + e_1 - e_2 + N,$$
$$\sigma(N) = -f(-1) = 1 + e_1 + e_2 + N.$$

The oracles can thus be used to deliver

$$2e_1 = \phi(N) + \sigma(N) - 2N, \qquad 2e_2 = \sigma(N) - \phi(N) - 2, \quad (7)$$

and the primes p_1, p_2, p_3 can now be recovered from $f(x) = 0$, either using the formula for the solutions to the cubic equation, or from the interval bisection method.

The case $N = p^2q$

The argument does not apply when the primes p_h are not distinct, because (5) is no longer valid. Consider the case when $N = p^2q$, where p, q are distinct primes to be found. We now have $\phi(p^2) = p^2 - p$, so that

$$\phi(N) = (p^2 - p)(q - 1) = N - p^2 - pq + p.$$

The term pq here can be eliminated by replacing it with N/p, delivering the cubic equation for p:

$$x^3 - x^2 - (N - \phi(N))x + N = 0. \quad (8)$$

Taking $\phi(N)$ from the oracle, the integer solution $x = p$ is then the required prime, and $q = N/p^2$.

https://doi.org/10.1017/mag.2019.113 Published online by Cambridge University Press

An example

Note that, in the previous two sections, the Σ-oracle is invoked only for the case when N is a product of three distinct primes. We state our results as a theorem and illustrate it with an example.

Theorem: Let N be a number with at most three not necessarily distinct prime divisors. If there are only two distinct prime divisors of N then, given the value of $\phi(N)$, the factorisation of N can be delivered in polynomial-time in $\log N$. If there are three distinct prime divisors of N then, given also the value of $\sigma(N)$, the factorisation of N can still be delivered in polynomial-time in $\log N$.

Let us take

$$N = 148859337163,$$

which is not a perfect power of an integer, as can be checked easily. For our purpose, we do not require a primality test for N. (The AKS test is efficient; see, for example, [1].) Instead, we ask the oracles to deliver for us

$$\sigma(N) = 148805922960, \qquad \sigma(N) = 148912769012,$$

and from $\phi(N) < N - 1$, we deduce that N has at least two distinct prime divisors.

Suppose first that $N = pq$, with $p < q$. This can be ruled out easily, without even considering the quadratic concerned. For example, by (6), we should have $\phi(N) + \sigma(N) = 2N + 2$, which is false.

Suppose next that $N = pqr$, with $p < q < r$. This can also be disposed of without considering the cubic concerned. Thus, by (7), $p + q + r = e_1 = 8823 < 9000$, which is too small because $N = pqr > 10^{11}$, so that the arithmetic-geometric means inequality for p, q, r is violated.

Thus, if N satisfies the hypothesis of the theorem, then $N = p^2 q$ with p, q being distinct primes, and the cubic in (8) is

$$x^3 - x^2 - 53414203x + 148859337163 = 0.$$

The integer root is $x = p = 3881$, and $q = N/p^2 = 9883$.

Summary

Because of the use of oracles, some readers may consider our theorem to be a somewhat vacuous statement, or perhaps a pointless exercise at best. However, integer factorisation is an active area of research and, as we already remarked, the use of oracles to study the complexity of a computational task is no idle pursuit. Indeed, the following theorem [2] is one of the current results related to our problem stated in the third section above.

https://doi.org/10.1017/mag.2019.113 Published online by Cambridge University Press

Theorem (Morain–Renault–Smith, 2018): Let N be a product of distinct primes, with the value of $\phi(N)$ also given. Suppose that there is a prime divisor p of N satisfying $p > \sqrt{N}$. Then p can be recovered in polynomial-time in $\log N$.

References

1. A. Granville, It is easy to determine whether a given number is prime, *Bull. Amer. Math. Soc.*, **42** (2005) pp. 3-38.
2. F. Morain, G. Renault, B. Smith, Deterministic factoring with oracles, https://hal.inria.fr/hal-01715832

10.1017/mag.2019.113
PETER SHIU
353 Fulwood Road, Sheffield S10 3BQ
e-mail: *p.shiu@yahoo.co.uk*

103.32 More on the gaps between sums of two squares

Introduction

In the Note [1], Peter Shiu presented some interesting results about the possible length of gaps between integers that are sums of two squares. Here we develop this investigation a little further. There are two main theorems in [1]. We will present a minor strengthening (apparently not previously known) of one of these theorems, and a greatly simplified (albeit weaker) version of the other.

Denote by Σ_2 the set of positive integers that are expressible as a sum of two squares. We allow one of the squares to be zero, so ordinary squares are included in Σ_2.

Our topic is the possible size of gaps between successive elements of Σ_2. A trivial starting observation is that gaps of length 1 occur infinitely often, since for each n, the numbers n^2 and $n^2 + 1$ are in Σ_2.

We review a few well-known facts about Σ_2.

(E1) No element of Σ_2 is congruent to 3 mod 4, since squares are congruent to 0 or 1 mod 4.

(E2) $2n \in \Sigma_2$ if, and only if, $n \in \Sigma_2$. We give the proof, since it is quick and easy. If $n = a^2 + b^2$, then $2n = (a + b)^2 + (a - b)^2$. Conversely, if $2n = a^2 + b^2$, then $(a + b)^2 = a^2 + b^2 + 2ab$ is even, so $a + b$ and $a - b$ are even, and we can express n as $\left[\frac{1}{2}(a + b)\right]^2 + \left[\frac{1}{2}(a - b)\right]^2$.

(E3) Prime numbers that are congruent to 1 mod 4 are in Σ_2. There are many ways to prove this. My favourite one was described in the *Gazette* Note [2].

(E4) $n \in \Sigma_2$ if, and only if, all primes that are congruent to 3 mod 4 occur to an even power in the factorisation of n. This builds on (E3), and is the standard characterisation of sums of two squares, e.g. see [3, Theorem 366].