A talk given at Huawei Company (Oct. 31, 2019)
and Shenzhen Univ. (Nov. 28, 2019)

Computability and Undecidability

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

Nov. 28, 2019

Abstract

In this talk we introduce the theory of computability and the undecidability results on Hilbert's Tenth Problem. We will also mention some algorithms concerning primes.

Part I. The Theory of Computability

Primitive recursive functions

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ and call each $n \in \mathbb{N}$ a *natural number*.

Three Basic Functions:

Zero Function: $O(x) = 0$ (for all $x \in \mathbb{N}$).

Successor Function: $S(x) = x + 1$.

Projection Function: $I_{nk}(x_1, \ldots, x_n) = x_k$ $(1 \leqslant k \leqslant n)$

Composition:

$$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$$

Primitive Recursion:

$$\begin{aligned} f(x_1, \ldots, x_n, 0) &= g(x_1, \ldots, x_n), \\ f(x_1, \ldots, x_n, y+1) &= h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)) \end{aligned}$$

Primitive recursive functions are the basic functions and those obtained from the basic functions by applying composition and primitive recursion a finite number of times.

Acknermann's function

It is easy to see that all primitive recursive functions are computable by our intuition.

Skolem's Claim (1924): All *intuitively computable* number-theoretic functions are primitive recursive functions.

In 1928 Ackermann showed that the following **Ackermann function** $A(m, n)$ is computable but not primitively recursive.

$$\begin{aligned} A(0, n) &= n + 1, \\ A(m + 1, 0) &= A(m, 1) \\ A(m + 1, n + 1) &= A(m, A(m + 1, n)). \end{aligned}$$

For example,

$$\begin{aligned} A(1, 2) &= A(0, A(1, 1)) = A(0, A(0, A(1, 0))) \\ &= A(0, A(0, A(0, 1))) = A(0, A(0, 2)) \\ &= A(0, 3) = 4. \end{aligned}$$

Partial recursive functions

μ-operator:

$$f(x_1, \ldots, x_n) = \mu y(g(x_1, \ldots, x_n, y) = 0)$$

means that $f(x_1, \ldots, x_n)$ is the least natural number y such that $g(x_1, \ldots, x_n, y) = 0$. If $g(x_1, \ldots, x_n, y) \neq 0$ for all $y \in \mathbb{N}$, then $f(x_1, \ldots, x_n)$ is undefined.

Partial recursive functions are the basic functions and those obtained from the basic functions by applying composition and μ-operator a finite number of times.

If a partial recursive function $f(x_1, \ldots, x_n)$ is defined for all $x_1, \ldots, x_n \in \mathbb{N}$, then f is called a *total recursive function*.

All primitive functions as well as the Ackermann function $A(m, n)$ are total recursive functions.

Church's Thesis

For any partial recursive function f, it is easy to see that if $f(x_1, \ldots, x_n)$ is defined then the value $f(x_1, \ldots, x_n)$ is effectively computable.

In 1936 A. Turing introduced the notion of Turing machine which is an abstract machine that manipulates symbols on a strip of tape according to a table of rules (i.e., a program). A function $f(x_1, \ldots, x_n)$ is Turing computable if there is a program according to which the Turing machine with initial inputs $x_1, \ldots, x_n$ finally stops and yields the value $f(x_1, \ldots, x_n)$ as outut if $f(x_1, \ldots, x_n)$ is defined, and never stops if $f(x_1, \ldots, x_n)$ is undefined.

Partial recursive functions and Turing computable functions were proved to be equivalent.

Church's Thesis (1936). If a function f into $\mathbb{N}$ with natural number variables is effectively computable by intuition, then it must be a partial recursive function (or a Turing computable function).

Recursively enumerable sets

A subset A of $\mathbb{N}$ is said to be an r.e. (recursively enumerable) set (or a semi-decidable set) if the function

$$f(x) = \begin{cases} 1 & \text{if } x \in A, \\ \text{undefined} & \text{if } x \in \mathbb{N} \setminus A. \end{cases}$$

is a partial recursive function.

If $A = \mathrm{Dom}(f)$ for some partial recursive function f, then we may revise the program computing $f(x)$ by letting the output be 1 if $f(x)$ is computed, and thus A is an r.e. set.

In view of the above,

$$\begin{aligned} & A \subseteq \mathbb{N} \text{ is an r.e. set} \\ \iff & A = \mathrm{Dom}(f) \text{ for some partial recursive function } f. \end{aligned}$$

Recursively enumerable sets

If A is an r.e. set containing an element a, and the program P computes the above function f, then the function

$$g(x,y) = \begin{cases} x & \text{if the program } P \text{ computes } f(x) \text{ within } y \text{ steps,} \\ a & \text{otherwise} \end{cases}$$

is a partial recursive function with $\mathrm{Ran}(g) = A$.

If A is the range of a partial recursive function $h(x_1, \ldots, x_n)$, then the function

$$f(x) = \begin{cases} 1 & \text{if } x \in \mathrm{Ran}(h) = A, \\ \text{undefined} & \text{otherwise,} \end{cases}$$

is a partial recursive function (we may seek for $x_1, \ldots, x_n$ with $h(x_1, \ldots, x_n)$ equal to a given $x \in A$), and thus A is an r.e. set.

So, a nonempty $A \subseteq \mathbb{N}$ is an r.e. set if and only if $A = \mathrm{Ran}(f)$ for some partial recursive function f.

r.e. sets and recursive sets

Enumeration Theorem. There is a partial recursive function $\varphi(m, n)$ such that

$$\varphi_0, \varphi_1, \varphi_2, \ldots$$

list all the partial recursive functions of one variable. where φ_m is given by

$$\varphi_m(n) = \varphi(m, n) \ (n = 0, 1, 2, \ldots).$$

A set $A \subseteq \mathbb{N}$ is called *decidable* or *recursive*, if the characteristic function

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \in \mathbb{N} \setminus A. \end{cases}$$

is Turing computable (or recursive).

A set $A \subseteq \mathbb{N}$ is recursive if and only if both A and $\mathbb{N} \setminus A$ are r.e. sets.

Halting Problem is undecidable

Theorem. The set $K = \{x \in \mathbb{N} : \ x \in \mathrm{Dom}(\varphi_x)\}$ is a nonrecursive r.e. set.

Proof. As the function $\varphi_x(x) = \varphi(x, x)$ is a partial recursive function, we see that K is an r.e. set.

Suppose that K is recursive. Then the function

$$f(x) = \begin{cases} \varphi_x(x) + 1 & \text{if } x \in \mathrm{Dom}(\varphi_x), \\ 0 & \text{otherwise,} \end{cases}$$

is totally recursive, thus for some $m \in \mathbb{N}$ we have $\varphi_m = f$ and hence

$$f(m) = \varphi_m(m) \neq \varphi_m(m) + 1$$

which leads a contradiction.

Let P_x be a Turing program computing φ_x. Whether a Turing machine with input x and program P_x finally stops, is an undecidable problem which is called the halting problem.

Part II. Solution to Hilbert's Tenth Problem

Hilbert's Tenth Problem

In 1900, at the Paris conference of ICM, D. Hilbert presented 23 famous mathematical problems. He formulated his tenth problem as follows:

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: `To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.`

In modern language, Hilbert's Tenth Problem (HTP) asked for an effective algorithm to test whether an arbitrary polynomial equation

$$P(z_1, \ldots, z_n) = 0$$

(with integer coefficients) has solutions over the ring $\mathbb{Z}$ of the integers.

However, at that time the exact meaning of algorithm was not known.

Diophantine equations over $\mathbb{N}$ and $\mathbb{Z}$

Throughout this talk, variables always range over $\mathbb{Z}$.

Let $P(z_1, \ldots, z_n) \in \mathbb{Z}[z_1, \ldots, z_n]$. Then

$$\begin{aligned} & \exists z_1 \ldots \exists z_n [P(z_1, \ldots, z_n) = 0] \\ \iff & \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 \left[\prod_{\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}} P(\varepsilon_1 x_1, \ldots, \varepsilon_n x_n) = 0 \right]. \end{aligned}$$

On the other hand, by Lagrange's four-square theorem (each $m \in \mathbb{N}$ can be written as the sum of four squares), we have

$$\begin{aligned} & \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 [P(x_1, \ldots, x_n) = 0] \\ \iff & \exists u_1 \exists v_1 \exists y_1 \exists z_1 \ldots \exists u_n \exists v_n \exists y_n \exists z_n \\ & [P(u_1^2 + v_1^2 + y_1^2 + z_1^2, \ldots, u_n^2 + v_n^2 + y_n^2 + z_n^2) = 0] \end{aligned}$$

So HTP has the following equivalent form (HTP over $\mathbb{N}$): *Is there an algorithm to decide for any polynomial $P(x_1, \ldots, x_n)$ with integer coefficients whether the Diophantine equation $P(x_1, \ldots, x_n) = 0$ has solutions with $x_1, \ldots, x_n \in \mathbb{N}$?*

Diophantine relations and Diophantine sets

A relation $R(a_1, \ldots, a_m)$ with $a_1, \ldots, a_m \in \mathbb{N}$ is said to be *Diophantine* if there is a polynomial $P(t_1, \ldots, t_m, x_1, \ldots, x_n)$ with integer coefficients such that

$$R(a_1, \ldots, a_m) \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 [P(a_1, \ldots, a_m, x_1, \ldots, x_n) = 0].$$

A set $A \subseteq \mathbb{N}$ is Diophantine if and only if the predicate $a \in A$ is Diophantine.

It is easy to see that any Diophantine set A is an r.e. set. In fact, for a given element $a \in A$ we may search for the natural number solutions of the related Diophantine equation. If it has a solution, then we will find one and let the computer stop and give the output 1. If it has no solution, the computer will never stop.

Davis Daring Hypothesis

In 1944 E. L. Post thought that HTP *begs for an unsolvability proof*, i.e., HTP might be undecidable.

In 1949 Martin Davis used Gödel's coding idea to obtain that any r.e. set $A \subseteq \mathbb{N}$ has the following Davis normal form

$$a \in A \iff \exists x \geqslant 0 \forall 0 \leqslant y \leqslant x \exists z_1 \geqslant 0 \ldots \exists z_n \geqslant 0 \\ [P(a, x, y, z_1, \ldots, z_n) = 0],$$

where a is a natural number and P is a polynomial with integer coefficients.

Davis Daring Hypothesis. Any r.e. set $A \subseteq \mathbb{N}$ is Diophantine.

Under this hypothesis, for the nonrecursive r.e. set $K = \{x \in \mathbb{N} : \ x \in \mathrm{Dom}(\varphi_x)\}$ there is a polynomial $P(x, x_1, \ldots, x_n)$ such that for any $a \in \mathbb{N}$ we have

$$a \in K \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 [P(a, x_1, \ldots, x_n) = 0].$$

Thus Davis Daring Hypothesis implies that HTP over $\mathbb{N}$ is undecidable.

Systems of Diophantine equations

A system of finitely many Diophantine equations is equivalent to a single Diophantine equation. In fact, if $P_i(z_1, \ldots, z_n) \in \mathbb{Z}[z_1, \ldots, z_n]$ for all $i = 1, \ldots, k$, then

$$\begin{aligned} & P_1(z_1, \ldots, z_n) = 0 \ \& \ \ldots \ \& \ P_k(z_1, \ldots, z_n) = 0 \\ \iff & P_1^2(z_1, \ldots, z_n) + \ldots + P_k^2(z_1, \ldots, z_n) = 0. \end{aligned}$$

The Davis-Putnam-Robinson Theorem

Theorem (M. Davis, H. Putnam, J. Robinson, Annals of Math. 1961) Any r.e. set is exponential Diophantine. Thus there is no algorithm to decide for any given exponential Diophantine equation whether it has solutions over $\mathbb{N}$.

Julia Robinson's Hypothesis

A. Tarski conjectured in 1948 that $\{2^n : \ n \in \mathbb{N}\}$ is not a Diophantine set. His PhD student J. Robinson did not succeed in proving this with serious efforts.

JR Hypothesis (J. Robinson, 1950). There is a Diophantine relation $R(a, b)$ with $a, b \in \mathbb{N}$ such that

$$R(a, b) \Rightarrow b < a^a$$

and

$$\forall k > 0 \exists a \geqslant 0 \exists b \geqslant 0 [R(a, b) \ \& \ a^k < b].$$

Under this hypothesis, J. Robinson showed that the exponential relation $a^b = c$ is Diophantine and hence all r.e. sets are Diophantine. So, the JR Hypothesis implies the negative solution of HTP.

J. Robinson tried to prove her JR Hypothesis but got no success. This made her depressed and doubt her Hypothesis.

Matiyasevich's Theorem

Recall that the Fibonacci sequence $(F_n)_{n\geqslant 0}$ defined by

$$F_0 = 0,\ F_1 = 1,\ \text{ and } F_{n+1} = F_n + F_{n-1}\ (n = 1, 2, 3, \ldots)$$

increases exponentially.
In 1970 Yu. Matiyasevich, a 23-year-old Russian, confirmed the JR Hypothesis by showing that the relation $y = F_{2x}$ (with $x, y \in \mathbb{N}$) is Diophantine! It follows the exponential relation $a^b = c$ (with $a, b, c \in \mathbb{N}$, $a > 1$ and $c > 0$) is Diophantine, i.e. there exists a polynomial $P(a, b, c, x_1, \ldots, x_n)$ with integer coefficients such that

$$a^b = c \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0[P(a, b, c, x_1, \ldots, x_n) = 0].$$

This, together with the Davis-Putnam-Robinson work in 1961, led Matiyasevich finally confirm Davis Daring Hypothesis.

Matiyasevich's Theorem (or MDPR Theorem) (1970).
Recursively enumerable sets coincide with Diophantine sets. Thus HTP has a negative solution!

Part III. Reduction of Natural Number Unknowns

Small ν with $\exists^\nu$ over $\mathbb{N}$ undecidable

For a set $S \subseteq \mathbb{Z}$ we let $\exists^n$ over S denote the set of formulas

$$\exists x_1 \in S \ldots \exists x_n \in S[P(x_1, \ldots, x_n) = 0]$$

with $P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$.

Any nonrecursive r.e. set A has a Diophantine representation:

$$a \in A \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0[P(x_1, \ldots, x_n) = 0].$$

It is interesting to find the least $\nu \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ such that $\exists^\nu$ over $\mathbb{N}$ is undecidable.

$\nu < 200$ (Matiyasevich, Summer of 1970)
$\nu \leqslant 35$ (J. Robinson, 1970)
$\nu \leqslant 24$ (Matiyasevich and Robinson, 1970)
$\nu \leqslant 14$ (Matiyasevich and Robinson, 1970)
$\nu \leqslant 13$ (Matiyasevich and Robinson, 1973 [Acta Arith. 27(1975)])
$\nu \leqslant 9$ (Matiyasevich, 1975; details in Jones [J. Symbolic Logic, 1982])

The 9 Unknowns Theorem

The above ideas, together with some other works in the 1975 paper of Matiyasevich and Robinson, led Mtijasevich obtain the following celebrated theorem.

Matiyasevich's 9 Unknowns Theorem: $\exists^9$ over $\mathbb{N}$ is undecidable!

The detailed proof of this theorem appeared in Jones [J. Symbolic Logic, 1982].

Up to now, no one has shown that $\exists^\nu$ over $\mathbb{N}$ is undecidable for some $\nu < 9$, although A.Baker, Matiyasevich and Robinson all believed that $\exists^3$ over $\mathbb{N}$ might be undecidable.

$\exists$ over $\mathbb{Z}$ is decidable

Matiyasevich and Robinson [Acta Arith. 27(1975)]: If $a_0, a_1, \ldots, a_n$ and z are integers with $a_0 z \neq 0$ and $\sum_{i=0}^{n} a_i z^{n-i} = 0$, then

$$|z|^n \leqslant |a_0 z^n| \leqslant \sum_{i=1}^{n} |a_i||z|^{n-i} \leqslant \sum_{i=1}^{n} |a_i||z|^{n-1}$$

and hence

$$|z| \leqslant \sum_{i=1}^{n} |a_i|.$$

Thus $\exists$ over $\mathbb{N}$ and $\exists$ over $\mathbb{Z}$ are decidable (in polynomial time).

It is not known whether $\exists^2$ over $\mathbb{Z}$ is decidable. But A. Baker proved in 1968 that if $P(x, y) \in \mathbb{Z}[x, y]$ is homogenous, irreducible and of degree at least three then for any $m \in \mathbb{Z}$ there is an effective algorithm to determine whether $P(x, y) = m$ for some $x, y \in \mathbb{Z}$.

Relative results

For any $m \in \mathbb{Z}$, by Lagrange's four-square theorem

$$m \geqslant 0 \iff \exists z_1 \exists z_2 \exists z_3 \exists z_4 [m = z_1^2 + z_2^2 + z_3^2 + z_4^2].$$

Thus

$$\exists^n \text{ over } \mathbb{N} \text{ is undecidable} \Rightarrow \exists^{4n} \text{ over } \mathbb{Z} \text{ is undecidable.}$$

By the Gauss-Legendre theorem on sums of three squares,

$$\mathbb{N} \setminus \{x^2 + y^2 + z^2 : \ x, y, z \in \mathbb{Z}\} = \{4^k(8l + 7) : \ k, l \in \mathbb{N}\}.$$

If $n \in \mathbb{N}$, then $4n + 1 = (2x)^2 + (2y)^2 + (2z + 1)^2$ for some $x, y, z \in \mathbb{Z}$, and hence $n = x^2 + y^2 + z^2 + z$. Thus, for any $m \in \mathbb{Z}$,

$$m \geqslant 0 \iff \exists x \exists y \exists z [m = x^2 + y^2 + z^2 + z].$$

It follows that

$$\exists^n \text{ over } \mathbb{N} \text{ is undecidable} \Rightarrow \exists^{3n} \text{ over } \mathbb{Z} \text{ is undecidable.}$$

Thus $\exists^{27}$ over $\mathbb{Z}$ is undecidable by the 9 unknowns theorem, as pointed out by S.P. Tung in [Japan J. Math., 11(1985)].

A new relation-combining theorem

Tung (1985) asked whether $\exists^\nu$ over $\mathbb{Z}$ is undecidable for some $\nu < 27$.

New Relation-Combining Theorem (Z.-W. Sun [Z. Math. Logik Grundlag. Math. 38(1992)]): Let $A_1, \ldots, A_k, B, C_1, \ldots, C_n, D, E$ be integers with $D \neq 0$. Then

$$\begin{aligned} & A_1, \ldots, A_k \in \square \wedge B \neq 0 \wedge C_1, \ldots, C_n \geqslant 0 \wedge D \mid E \\ \Longleftrightarrow\ & \exists z_1 \ldots \exists z_{n+2} [P(A_1, \ldots, A_k, B, C_1, \ldots, C_n, D, E, z_1, \ldots, z_{n+2}) = 0], \end{aligned}$$

where P is a suitable polynomial with integer coefficients.

This implies that

$$\exists^n \text{ over } \mathbb{N} \text{ is undecidable} \Rightarrow \exists^{2n+2} \text{ over } \mathbb{Z} \text{ is undecidable.}$$

So $\exists^{20}$ over $\mathbb{Z}$ is undecidable by the 9 unknowns theorem.

$\exists^{11}$ over $\mathbb{Z}$ is undecidable

In 1992, I announced that $\exists^{11}$ **over** $\mathbb{Z}$ **is undecidable**.

To achieve this goal, unlike others I did not simply use the relative result, instead I adapt the deep proof of the 9 unknowns theorem and made suitable variants so that we can use integer variables instead of natural number variables.

My starting point is the use of Lucas sequences with integer indices instead of the usual natural number indices. I published this initial step in Sci. China Ser. A 35(1992).

The whole proof of the undecidability of $\exists^{11}$ over $\mathbb{Z}$ is very sophisticated. It appeared in my PhD thesis in 1992. During 1992-2016, despite that many mathematicians wanted to see my detailed proof, I did not write an English version of that, since I was frequently busy with my new discoveries.

After 25 years have passed, I finally spent time to write an English paper which contains the undecidability of $\exists^{11}$ over $\mathbb{Z}$ as well as my new discoveries related to HTP. The preprint is now publicly available from `http://arxiv.org/abs/1704.03504`

Part III. Some Algorithms involving Primes

Initial Results on Discriminants

Theorem 1 (L. K. Arnold, S. J. Benkoski and B. J. McCabe [Amer. Math. Monthly 92 (1985), no. 4]). Let $n > 4$ be an integer. Then the least positive integer m (denoted by $D(n)$) such that $1^1, 2^2, \ldots, n^2$ are distinct modulo m, is

$$\min\{m \geqslant 2n : \ m = p \text{ or } m = 2p \ \text{ with } p \text{ an odd prime}\}.$$

Remark. The range of $D(n)$ does not contain those primes $p = 2q + 1$ with q an odd prime.

The theorem arose from consideration of a problem in computer simulation. The problem may be described as developing a method to determine quickly the square roots of a long sequence of integers. For a long sequence $1^2, 2^2, \ldots, n^2$ of squares, you may use the function $A(x) = \sqrt{x}$ $(1 \leqslant x \leqslant n^2)$ to get the square roots. This needs an array of size $1 \times n^2$. If $1^2, 2^2, \ldots, n^2$ are distinct modulo m, then letting $A(r) = \sqrt{x}$ where $r \in \{1, \ldots, m\}$ and $r \equiv x \pmod{m}$. The modulo procedure is , in general, much faster than the square root procedure.

Generate all primes in a combinatorial manner

Theorem 1 (Sun, Feb. 29, 2012) (i) For $n \in \mathbb{Z}^+$ let $S(n)$ denote the smallest integer $m > 1$ such that those $2k(k-1) \bmod m$ for $k = 1, \ldots, n$ are pairwise distinct. Then $S(n)$ is the least prime greater than $2n-2$.

(ii) For $n \in \mathbb{Z}^+$ let $T(n)$ denote the least integer $m > 1$ such that those $k(k-1) \bmod m$ with $1 \leqslant k \leqslant n$ are pairwise distinct. Then we have

$$T(n) = \min\{m \geqslant 2n-1 : \ m \text{ is a prime or a positive power of } 2\}.$$

Remark. (a) **The range of $S(n)$ is exactly the set of all primes!** (b) I proved that the least positive integer m such that those $\binom{k}{2} = k(k-1)/2$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m, is just the least power of two not smaller than n.

Another theorem

Theorem 2 (Sun, March 2012) (i) Let $d \in \{2, 3\}$ and $n \in \mathbb{Z}^+$. Then the smallest positive integer m such that those $k(dk-1)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m, is the least power of d not smaller than n.

(ii) Let $n \in \{4, 5, \ldots\}$. Then the least positive integer m such that $18k(3k-1)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m, is just the least prime $p > 3n$ with $p \equiv 1 \pmod 3$.

Remark. We are also able to prove some other similar results; for example, for each $n > 5$ the least $m \in \mathbb{Z}^+$ such that those $18k(3k+1)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m, is just the first prime $p \equiv -1 \pmod 3$ after $3n$.

Alternating sums of primes

Let p_n be the nth prime and define

$$s_n = p_n - p_{n-1} + \cdots + (-1)^{n-1} p_1.$$

Note that

$$s_{2n} = \sum_{k=1}^{n} (p_{2k} - p_{2k-1}) > 0, \quad s_{2n+1} = \sum_{k=1}^{n} (p_{2k+1} - p_{2k}) + p_1 > 0.$$

Here are values of $s_1, \ldots, s_{16}$:

$$2,\ 1,\ 4,\ 3,\ 8,\ 5,\ 12,\ 7,\ 16,\ 13,\ 18,\ 19,\ 22,\ 21,\ 26,\ 27.$$

The sequence $0, s_1, s_2, \ldots$ were first introduced by N.J.A. Sloane and J.H. Conway (see A008347 at OEIS).

It is not difficult to show that those s_n $(n = 1, 2, 3, \ldots)$ are pairwise distinct.

An amazing recurrence for primes

The following surprising conjecture on recurrence for primes allows us to compute p_{n+1} in terms of $p_1, \ldots, p_n$.

Conjecture (Sun, March 28, 2012). For any positive integer $n \neq 1, 2, 4, 9$, the $(n+1)$th prime p_{n+1} is the least positive integer m such that

$$2s_1^2, \ldots, 2s_n^2$$

are pairwise distinct modulo m.

Remark. I have verified the conjecture for $n \leqslant 2 \times 10^5$, and proved that $2s_1^2, \ldots, 2s_n^2$ **are indeed pairwise distinct modulo** p_{n+1}.

A Related Conjecture (Sun, March 26, 2012). The least integer $m > 1$ such that $2S_k^2$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m is a prime smaller than n^2 unless $n \mid 6$, where $S_k = \sum_{j=1}^{k} p_j$.

Conjecture on alternating sums of consecutive primes

Conjecture (Sun, April 2-3, 2012). For any positive integer m, there are consecutive primes $p_k, \ldots, p_n$ $(k \leqslant n)$ not exceeding $2m + 2.2\sqrt{m}$ such that

$$m = p_n - p_{n-1} + \cdots + (-1)^{n-k} p_k.$$

Examples.

$$10 = 17 - 13 + 11 - 7 + 5 - 3;$$
$$20 = 41 - 39 + 37 - 31 + 29 - 23 + 19 - 17 + 13 - 11;$$
$$2382 = p_{652} - p_{651} + \cdots + p_{44} - p_{43},$$
$$p_{652} = 4871 = \lfloor 2 \cdot 2382 + 2.2\sqrt{2382} \rfloor.$$

The conjecture has been verified for m up to 10^9. Most known results on primes are about local properties of primes, not about relations of primes.

Prize. I would like to offer 1000 US dollars for the first proof.

How to solve $x^2 \equiv a \pmod{p}$?

Let p be an odd prime and a be any quadratic residue modulo p. How to solve the congruence $x^2 \equiv a \pmod{p}$ quickly?

Tonelli-Shanks Algorithm. Knowing a *quadratic nonresidue* $d \in \mathbb{Z} \bmod p$, one can solve $x^2 \equiv a \pmod{p}$ in **polynomial time**:

Write $p - 1 = 2^s t$ with $s, t \in \mathbb{Z}^+$ and $2 \nmid t$, and find even integers $m_1, \ldots, m_s$ with $(ad^{m_i})^{2^{s-i}t} \equiv 1 \pmod{p}$ for all $i = 1, \ldots, s$ in the following way: $m_1 := 0$, and after those $m_1, \ldots, m_i$ (with $1 \leqslant i < s$) have been chosen we select $m_{i+1} \in \{m_i, m_i + 2^i\}$ such that $(ad^{m_{i+1}})^{2^{s-i-1}t} \equiv 1 \pmod{p}$. Note that $((ad^{m_i})^{2^{s-i-1}t})^2 \equiv 1 \pmod{p}$ and hence $(ad^{m_i})^{2^{s-i-1}t} \equiv \pm 1 \pmod{p}$. If $(ad^{m_i})^{2^{s-i-1}t} \equiv -1 \pmod{p}$, then

$$(ad^{m_i+2^i})^{2^{s-1-i}t} \equiv -d^{2^{s-1}t} = -d^{(p-1)/2} \equiv 1 \pmod{p}.$$

As $(ad^{m_s})^t \equiv 1 \pmod{p}$, we have $x^2 \equiv a \pmod{p}$ with $x = \pm a^{(t+1)/2}(d^t)^{m_s/2}$.

Remark. In 1985 R. Schoof gave a polynomial (depending on a) algorithm to solve the congruence $x^2 \equiv a \pmod{p}$ with a given.

Find a quadratic nonresidue modulo a prime

However, there is no known deterministic, polynomial time algorithm for finding a quadratic nonresidue d modulo the odd prime p. Under the Extended Riemann Hypothesis for algebraic fields, it can be shown that there is a positive quadratic nonresidue $d < 2\log^2 p$; and so an exhaustive search to this limit succeeds in finding a quadratic nonresidue in polynomial time.

As Fibonacci numbers grow exponentially, our following conjecture is particularly interesting since it implies that we can find square roots for quadratic residues modulo any odd prime p in deterministic, polynomial time.

Conjecture (Z.-W. Sun, 2014) For any integer $n > 4$, there is a Fibonacci number $f < n/2$ with $x^2 \equiv f \pmod{n}$ for no integer x.

Remark. This can be reduced to the case with $n = p$ prime. We have verified that for any prime $3 < p < 3 \times 10^9$ there is a Fibonacci number $F_k < p/2$ with $(\frac{F_k}{p}) = -1$.

The partition function $p(n)$

A *partition* of a positive integer n is a way to write n as a sum of positive integers with the order of addends ignored. The partition function $p(n)$ denotes the total number of partitions of n.

Example. $p(5) = 7$ since

$$\begin{aligned} 5 =& 1+4 = 2+3 = 1+1+3 = 1+2+2 \\ =& 1+1+1+2 = 1+1+1+1+1. \end{aligned}$$

Hardy-Ramanujan Formula:

$$p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4\sqrt{3}n} \quad \text{as } n \to +\infty,$$

and hence

$$\log p(n) \sim c\sqrt{n} \ \text{ with } c = \pi\sqrt{\frac{2}{3}}.$$

Note that $p(n)$ grows eventually faster than any polynomial in n but slightly slower than 2^n. `Mathematica` could compute $p(n)$ quickly.

On primes related to $p(n)$

Conjecture 1 (Sun, 2014-02-27). Let n be any positive integer. Then one of the n numbers

$$p(n)+1,\ p(n)+2,\ \ldots,\ p(n)+n$$

is prime.

Conjecture 2 (Sun, 2014-02-28). Let $n>1$ be an integer. Then $p(n)+p(k)-1$ is prime for some $0<k<n$.

Conjecture 3 (Sun, 2014-03-13). Let $n>3$ be an integer. Then $p(n+k)+1$ is prime for some $k=1,\ldots,n$.

Conjecture 4 (Sun, 2014-03-12). Let $n>1$ be an integer. Then there exists a number $k\in\{1,\ldots,n-1\}$ such that $kp(n)(p(n)-1)+1$ is prime. Also, we may replace $kp(n)(p(n)-1)+1$ by $p(k)p(n)(p(n)-1)+1$ or $p(k)p(n)(p(n)+1)-1$.

These conjectures might be helpful in finding large primes for the use of RSA.

References

For main sources of my work mentioned here, you may look at:

1. Z.-W. Sun, *Reduction of unknowns in Diophantine representations*, Sci. China Math. 35(1992), 257–269.

2. Z.-W. Sun, *A new relation-combining theorem and its application*, Z. Math. Logik Grundlag. Math. 38(1992), 209-212.

3. Z.-W. Sun, *Further results on Hilbert's tenth problem*, arXiv:1704.03504, http://arxiv.org/abs/1704.03504.

4. Z.-W. Sun, *On functions taking only prime values*, J. Number Theory 133 (2013), 2794–2812.

5. Z.-W. Sun, *Problems on combinatorial properties of primes*, in: M. Kaneko, S. Kanemitsu and J. Liu (eds.), Number Theory: Plowing and Starring through High Wave Forms, Proc. 7th China-Japan Seminar (Fukuoka, Oct. 28–Nov. 1, 2013), Ser. Number Theory Appl., Vol. 11, World Sci., Singapore, 2015, pp. 169-187.

Thank you!