What can we prove?

Here is a proposition of first-order arithmetic:

$\forall x \exists y \exists z (Prime(y) \wedge Prime(z) \wedge y + z = ss0 * ssx)$

where

$Prime(x) \equiv \forall y \forall z (y * z = x \rightarrow (y = s0 \leftrightarrow \neg z = s0))$

(i.e., "Every even number greater than 2 is the sum of two primes").

This is *Goldbach's Conjecture* (GC).

Consider these questions:

1. Is GC a theorem of Peano arithmetic (PA)? (Currently unknown)

2. Is GC a theorem of any sound formal system for arithmetic? (Currently unknown)

3. Is GC true? (Currently unknown)

Further questions

1. If GC is true, must it be a theorem of Peano arithmetic? (Only if PA is complete — i.e., its theorems include all true first-order arithmetical statements)

2. If GC is a theorem of Peano arithmetic, must it be true? (Only if PA is sound — i.e., all its theorems are true)

3. If GC is true, must it be a theorem of *some* sound formal system of arithmetic? (Only if there is a sound and complete formal system for arithmetic).

PA *is* sound. But it is not complete.

We know this because Gödel proved that *there cannot be a formal system for arithmetic that is both sound and complete.*

Gödel's proof: a sketch

Assume we have a formal system S for first-order arithmetic. The *standard interpretation* of formula ϕ is an arithmetical proposition p_ϕ. The *Gödelian interpretation* is a statement q_ϕ about S, such that q_ϕ is true iff p_ϕ is true.

The Gödel formula γ has Gödelian interpretation "γ is not provable in S". It also has a standard interpretation p_γ.

If p_γ is true, so is q_γ, so γ is not provable in S. Some true arithmetical statement is not provable in S: *S is not complete.*

If p_γ is false, so is q_γ, so γ is provable in S. Some formula provable in S is arithmetically false: *S is not sound.*

Hence S is not both sound and complete.

The logical language

We shall work with a pared-down logical language, consisting of just 12 symbols, which is capable of representing all formulae of first-order arithmetic.

The only logical constants we use are '$\neg$', '$\vee$' and $\forall$. The others can be defined by

$$\begin{aligned}
\phi \wedge \psi &\equiv \neg(\neg\phi \vee \neg\psi) \\
\phi \rightarrow \psi &\equiv \neg\phi \vee \psi \\
\phi \leftrightarrow \psi &\equiv \neg(\neg\phi \vee \neg\psi) \vee \neg(\phi \vee \psi) \\
\exists x \phi &\equiv \neg\forall x \neg\phi
\end{aligned}$$

We use '0', 's', '=', '+', '×' as in first-order arithmetic.

Symbols 'x' and '$'$' enable us to build up as many variables as we need:

$$x, x', x'', x''', x'''', x''''', \ldots$$

Finally, we shall use parentheses '(' and ')'.

Example

Goldbach's Conjecture

$$\begin{aligned}
&\forall x \exists y \exists z(\\
&\quad \forall t \forall u (u * t = y \rightarrow (u = s0 \leftrightarrow \neg t = s0)) \\
&\quad \wedge\ \forall t \forall u (u * t = z \rightarrow (u = s0 \leftrightarrow \neg t = s0)) \\
&\quad \wedge\ y + z = ss0 * ssx)
\end{aligned}$$

can be simplified to

$$\begin{aligned}
&\forall x \exists y \exists z(\\
&\quad \forall t \forall u ((u * t = y \vee u * t = z) \\
&\qquad \rightarrow\ (u = s0 \leftrightarrow \neg t = s0)) \\
&\quad \wedge\ y + z = ss0 * ssx)
\end{aligned}$$

which can be written in the pared-down notation as

$$\begin{aligned}
&\forall x \neg \forall x' \forall x''(\\
&\quad \neg \forall x''' \forall x''''(\\
&\qquad \neg(x''' * x'''' = x' \vee x''' * x'''' = x'') \\
&\qquad \vee\ (\neg(\neg x''' = s0 \vee t = s0) \\
&\qquad\quad \vee\ \neg(x''' = s0 \vee \neg t = s0))) \\
&\quad \vee\ \neg x' + x'' = ss0 * ssx)
\end{aligned}$$

Gödel Numbering

Assign numbers to the primitive symbols of the language:

0	s	=	¬	∨	∀	(	)	+	*	x	′
1	3	5	7	9	11	13	15	17	19	21	23

Assign numbers to formulae:

$$\forall x\ x = x$$

corresponds to the string 11, 21, 21, 5, 21 which is encoded as the integer

$$2^{11} \times 3^{21} \times 5^{21} \times 7^{5} \times 11^{21}$$

The formula can be recovered from the unique prime factorisation of this number.

Gödel numbers of sequences

A sequence of formulae (such as might constitute a proof, for example) can similarly be encoded.

The Gödel number of the sequence

$$\phi_1, \phi_2, \phi_3, \phi_4, \ldots, \phi_n$$

is

$$2^{g(\phi_1)} \times 3^{g(\phi_2)} \times 5^{g(\phi_3)} \times 7^{g(\phi_4)} \times \cdots p_n^{g(\phi_n)},$$

where $g(\phi)$ is the Gödel number of ϕ and p_n is the nth prime number.

Properties of formulae encoded as computable properties of their Gödel numbers

A formula is a universal generalisation iff its Gödel number is divisible by 2^{11} *but not by* 2^{12}.

A formula is a negation iff its Gödel number is divisible by 2^7 *but not by* 2^8.

Formula ϕ is an initial substring of formula ψ iff $g(\psi) = k.g(\phi)$, where k and $g(\phi)$ have no common factors.

These are simple examples, but Gödel showed that many logical properties of formulae (and sequences of formulae such as proofs) correspond to computable arithmetical properties of their Gödel numbers.

Some examples are given on the next slide.

Some logical properties of formulae for which the corresponding arithmetical properties of their Gödel numbers are computable:

ϕ is the negation of ψ.

ϕ is the formula obtained from ψ by substituting a given term for all free occurrences of a given variable.

ϕ is a conditional, ψ is its antecedent, and χ is its consequent.

χ is an immediate consequence of ϕ and ψ.

$\phi_1, \phi_2, \ldots, \phi_n$ is a valid proof in the system.

ϕ is provable in the system.

Constructing the Gödel Formula I

First construct a formula $Pf(x, y)$ which says that
(i) x is the Gödel number of a formula $\phi(z)$ with one free variable, and
(ii) y is the Gödel number of a proof of the formula $\phi(x)$.

Next consider the formula

$$\forall y \neg Pf(x, y).$$

This has one free variable, x.
Abbreviate it $\beta(x)$, and let its Gödel number be g.

$\beta(x)$ says that for any y, it is not the case that y is the Gödel number of a proof in S of the formula $\phi(x)$, where x is the Gödel number of the open formula $\phi(z)$.

Constructing the Gödel Formula II

Consider the formula $\beta(g)$, i.e., $\forall y \neg Pf(g, y)$. This says:

(1) For each y, it is not the case that g is the Gödel number of a formula $\phi(x)$ containing one free variable, such that y is the Gödel number of a proof, in S, of the formula $\phi(g)$.

Since g is the Gödel number of $\beta(x)$, we can simplify (1) to:

(1′) For each y, it is not the case that y is the Gödel number of a proof, in S, of the formula $\beta(g)$.

More simply still, $\beta(g)$ says that

(1″) $\beta(g)$ cannot be proved in S.

Thus the formula $\beta(g)$ asserts its own unprovability in S; it is therefore a Gödel formula for the formal system S.

A complete set of axioms for the first-order arithmetic of the real numbers

1. $x + (y + z) = (x + y) + z$
2. $x + y = y + x$
3. $x + 0 = x$
4. $x + (-x) = 0$
5. $x * (y * z) = (x * y) * z$
6. $x * y = y * x$
7. $x * 1 = x$
8. $x \neq 0 \rightarrow x * x^{-1} = 1$
9. $x * (y + z) = (x * y) + (x * z)$
10. $0 \neq 1$
11. $0^{-1} = 0$
12. $0 \leq x \vee 0 \leq (-x)$
13. $0 \leq x \wedge 0 \leq (-x) \rightarrow x = 0$
14. $0 \leq x \wedge 0 \leq y \rightarrow 0 \leq x + y$
15. $0 \leq x \wedge 0 \leq y \rightarrow 0 \leq x * y$
16. $x \leq y \leftrightarrow 0 \leq y + (-x)$
17. $\exists x \Phi(x) \wedge \exists y \forall x (\Phi(x) \rightarrow x \leq y)$
    $\rightarrow \exists z \forall y (\forall x (\Phi(x) \rightarrow x \leq y) \leftrightarrow z \leq y)$