PRATT'S PRIMALITY PROOFS

(Lecture notes written by Vašek Chvátal)

A theorem. It is a fact that an integer m greater than 2 is a prime if and only if there is an integer a such that

$$a^{m-1} \equiv 1 \pmod{m} \tag{1}$$

and

$$a^x \not\equiv 1 \pmod{m} \text{ for all } x = 1, 2, \ldots, m-2. \tag{2}$$

(Such an a is referred to as the *primitive root* of the prime m.)

How to use the theorem: an illustration. To illustrate a use of this fact, let us certify primality of 1783 by proving that

$$10^{1782} \equiv 1 \pmod{1783} \tag{3}$$

and that

$$10^x \not\equiv 1 \pmod{1783} \text{ for all } x = 1, 2, \ldots, 1781 \tag{4}$$

Having verified (3), we do not have to compute the 1781 values of 10^x mod 1783 in order to verify (4). Instead, we observe that $1782 = 2 \cdot 3^4 \cdot 11$ and then we evaluate only

$$\begin{aligned} 10^{1782/2} \bmod 1783 &= 10^{891} \bmod 1783 &&= 1782, \\ 10^{1782/3} \bmod 1783 &= 10^{594} \bmod 1783 &&= 1589, \\ 10^{1782/11} \bmod 1783 &= 10^{162} \bmod 1783 &&= 367. \end{aligned}$$

To see that (4) follows, let x denote the smallest positive integer such that $10^x \equiv 1 \pmod{1783}$. With c, d the integers defined by $cx + d = 1782$ and $0 \le d < x$ (specifically, $c = \lfloor 1782/x \rfloor$ and $d = 1782 \bmod x$), we have $10^{cx+d} = 10^{1782} \equiv 1 \pmod{1783}$ and $10^{cx} = (10^x)^c \equiv 1 \pmod{1783}$; it follows that $10^d \equiv 1 \pmod{1783}$; since $0 \le d < x$, minimality of x implies $d = 0$, and so x divides 1782. Since $10^{1782/2} \not\equiv 1 \pmod{1783}$, x does not divide $3^4 \cdot 11$; since $10^{1782/3} \not\equiv 1 \pmod{1783}$, x does not divide $2 \cdot 3^3 \cdot 11$; since $10^{1782/11} \not\equiv 1 \pmod{1783}$, x does not divide $2 \cdot 3^4$; we conclude that $x = 1782$.

A formal proof system. More generally, having verified (1), we do not have to compute the $m-2$ values of $a^x \bmod m$ in order to verify (2). Instead, we only need verify that $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ for all prime divisors p of $m-1$. This observation leads to a formal proof system with two kinds of theorems, namely,

m,

interpreted as "m is a prime" and

(m, a, x),

interpreted as "each prime divisor p of x satisfies $a^{(m-1)/p} \not\equiv 1 \pmod{m}$". This formal system consists of one class of axioms, namely,

$(m, a, 1)$ for all choices of positive integers m and a,

and two inference rules, namely,

$(m, a, x), p \vdash (m, a, xp)$

as long as $a^{(m-1)/p} \not\equiv 1 \pmod{m}$,

and

$(m, a, m-1) \vdash m$

as long as $a^{m-1} \equiv 1 \pmod{m}$.

For instance, the following sequence constitutes a formal proof of primality of 1783:

(S1)	(2,1,1)	axiom	
(S2)	2	from (S1)	since $1^1 \equiv 1 \pmod 2$
(S3)	(3,2,1)	axiom	
(S4)	(3,2,2)	from (S3) and (S2)	since $2^{2/2} \equiv 2 \pmod 3$
(S5)	3	from (S4)	since $2^2 \equiv 1 \pmod 3$
(S6)	(5,2,1)	axiom	
(S7)	(5,2,2)	from (S6) and (S2)	since $2^{4/2} \equiv 4 \pmod 5$
(S8)	(5,2,4)	from (S7) and (S2)	since $2^{4/2} \equiv 4 \pmod 5$
(S9)	5	from (S8)	since $2^4 \equiv 1 \pmod 5$
(S10)	(11,2,1)	axiom	
(S11)	(11,2,2)	from (S10) and (S2)	since $2^{10/2} \equiv 10 \pmod{11}$
(S12)	(11,2,10)	from (S11) and (S9)	since $2^{10/5} \equiv 4 \pmod{11}$
(S13)	11	from (S12)	since $2^{10} \equiv 1 \pmod{11}$
(S14)	(1783,10,1)	axiom	
(S15)	(1783,10,2)	from (S14) and (S2)	since $10^{1782/2} \equiv 1782 \pmod{1783}$
(S16)	(1783,10,6)	from (S15) and (S5)	since $10^{1782/3} \equiv 1589 \pmod{1783}$
(S17)	(1783,10,18)	from (S16) and (S5)	since $10^{1782/3} \equiv 1589 \pmod{1783}$
(S18)	(1783,10,54)	from (S17) and (S5)	since $10^{1782/3} \equiv 1589 \pmod{1783}$
(S19)	(1783,10,162)	from (S18) and (S5)	since $10^{1782/3} \equiv 1589 \pmod{1783}$
(S20)	(1783,10,1782)	from (S19) and (S13)	since $10^{1782/11} \equiv 367 \pmod{1783}$
(S21)	1783	from (S20)	since $10^{1782} \equiv 1 \pmod{1783}$

A nice upper bound on the length of proofs. Easy induction shows that

($\star$) primality of any prime m can be proved in at most $6 \lg m - 4$ lines.

Let us spell out the details. Lines (S1) and (S2) prove primality of 2; lines (S1) through (S5) prove primality of 3; since $6 \lg 2 - 4 = 2$ and since $3^6 > 2^9$, claim ($\star$) holds for $m = 2$ and $m = 3$. If m is any larger prime, then $m - 1$ is composite, and so there are (not necessarily distinct) primes $p_1, p_2, \ldots, p_k$ such that $k \geq 2$ and such that $m - 1 = p_1 p_2 \ldots p_k$. A proof of primality of m consists of proofs of primality of these (at most k) primes followed by the $k + 2$ lines

$$(m, a, 1),\ (m, a, p_1),\ (m, a, p_1 p_2),\ \ldots, (m, a, p_1 p_2 \ldots p_k),\ m;$$

the induction hypothesis guarantees that the entire proof consists of at most

$$\sum_{i=1}^{k}(6\lg p_i - 4) + k + 2$$

lines; the induction step is completed by observing that

$$\sum_{i=1}^{k}(6\lg p_i - 4) + k + 2 = 6\lg(m-1) - 3k + 2 \leq 6\lg(m-1) - 4.$$

Checking the proofs. Short proofs may be difficult to check. But the proofs discussed here are not: verifying each line other than an axiom takes evaluating some $a^n \bmod m$. The number of multiplications mod m required to do that does not exceed twice the number of bits in the binary encoding of n. Here is how it can be done:

```
u = a, v = n, w = 1;
while v > 0
do    if    v is even
      then  u = u^2 mod m, v = v/2;
      else  w = uw mod m, v = v - 1;
      end
end
return w;
```

The invariant preserved by each execution of the body of the **while** loop is

$$w \cdot u^v \equiv a^n \pmod{m}.$$

What is the point of all this? The problem of recognizing primes belongs to NP.

And isn't that
a fine thing
to know.

_____*****_____

These notes are based on

V. R. Pratt, "Every prime has a succinct certificate", *SIAM J. Computing* **4** (1975), 214–220.