Primality tests: An infinity of exceptions

As the consummate escape artist of his generation, magician Harry Houdini was famous for slipping out of what looked like inescapable predicaments — even when tightly bound, handcuffed, and locked in a trunk. Certain numbers display a similar slipperiness, eluding the ingenious snares set by mathematicians bent on distinguishing prime numbers from composite numbers as quickly and efficiently as possible.

So-called Carmichael numbers rank at the top of the sneakiness chart. Though rare, they can confound tests based on Pierre de Fermat's "little theorem," passing for prime numbers — those divisible only by themselves and one — when they really represent several smaller numbers multiplied together.

Now a trio of mathematicians at the University of Georgia in Athens has proved there are infinitely many Carmichael numbers. Their proof settles an issue that dates back to 1910, when mathematician R.D. Carmichael first uncovered such numbers, computed 15 examples, and stated without proof that "this list might be indefinitely extended."

The new proof, which represents the work of William R. (Red) Alford, Andrew Granville, and Carl Pomerance, also highlights the intrinsic inadequacy of certain types of tests employed within various widely used commercial computer programs for rapidly verifying that a given number is prime. Knowing whether a number is prime plays a key role in several cryptographic schemes for assuring computer security (SN: 9/7/91, p.148).

"The result itself is not surprising," says mathematician Hugh C. Williams of the University of Manitoba in Winnipeg. "What's interesting is that now there is a proof, and the proof is actually quite short, very elegant, very clever."

Granville describes the steps leading to the proof in the September NOTICES OF THE AMERICAN MATHEMATICAL SOCIETY.

The simplest way of determining primality is by trial division — dividing the given number by every number between 2 and the square root of the given number. If these trial divisors all leave a remainder, then the given number must be a prime. That's easy to do with small numbers, such as 107 or 11,035, but impossibly time-consuming for, say, 100-digit numbers.

In 1640, Fermat noticed a certain arithmetical relationship that pointed to a potential shortcut for culling lists of numbers. He discovered that if a number n is prime, then n divides evenly into $b^n - b$. Thus, for $n = 11$ and $b = 2$, $2^{11} - 2 = 2{,}046$, and 11 divides evenly into 2,046. This works for all prime numbers.

If there is a remainder, the given number is composite. However, a few composite numbers also leave no remainder for one or more choices of b, and Carmichael numbers comprise those even rarer composite numbers that pass as prime numbers no matter what value of b is chosen.

In other words, Fermat's test provides a remarkably efficient means of establishing that a given number hundreds of digits long is composite. But because certain numbers slip through, it can't serve as a definitive test of primality.

"This has made things very frustrating for primality testers," Williams says. "Although we have ways now of getting around this, it turns out the nicest, simplest way of attempting to get a primality test fails utterly because of the Carmichael numbers."

How common are Carmichael numbers? The smallest is 561. There are only 43 smaller than 1 million, and a total of 105,212 among the first 10^{15} whole numbers.

Until the beginning of this year, Carmichael numbers seemed both scarce and hard to find. Then Alford discovered a surprisingly simple, practical method for identifying Carmichael numbers in vast quantities. "He found a way to produce huge numbers of Carmichael numbers with hardly any work," Pomerance says. "It worked out beautifully."

The ease with which it was possible to demonstrate the existence of so many Carmichael numbers spurred Alford's colleagues to return to the long-standing question of whether there was an unlimited supply of these numbers. "Certain faculty members, here at the University of Georgia, taunted the number theory group that . . . surely Alford's idea should provide sufficient impetus to finally prove that there are infinitely many Carmichael numbers," Granville says. "And indeed it did."

Filling in the details of the resulting proof required sophisticated techniques and special theorems drawn from several fields of mathematics. "Maybe with this theorem under our belts, it may be possible for us or other people to start finding examples . . . of composite numbers that would also get through [other] tests," Pomerance notes. — *I. Peterson*

Twins offer key to genetics of smoking

Genes may help explain why some youths who experiment with cigarettes quickly develop a lifelong addiction while others can abstain from smoking or drop the habit easily. However, few studies have gauged the magnitude of such genetic effects or isolated where they may function in initiating, maintaining, or abandoning the cigarette habit. A new study now suggests that genes exert a moderate influence on all aspects of smoking — even on how much one smokes.

From 1967 to 1969, and again from 1983 to 1985, the National Heart, Lung, and Blood Institute in Bethesda, Md., surveyed male twins — both identical and fraternal pairs — born between 1917 and 1927. The survey included questions on such heart-disease risks as smoking.

Because these men had all served in the military during World War II — an environment in which cigarette smoking was common, even encouraged — this proved a group "maximally exposed to smoke," notes Dorit Carmelli of SRI International in Menlo Park, Calif., who led the new study. That's important, she says, because people must have the opportunity to smoke before any genetic influence can appear.

That pairs of identical twins (who have nearly identical genes) proved significantly more likely than pairs of fraternal twins to share the same smoking history strongly indicates a genetic role in cigarette addiction, her team reports in the Sept. 17 NEW ENGLAND JOURNAL OF MEDICINE.

Data on smoking intensity among these 4,775 pairs of twins proved "surprising — and encouraging from the potential for intervention," Carmelli says. Specifically, her team found no evidence that family environment affected how many cigarettes a man smoked. And genes appeared to influence intensity only at the extremes: in men smoking more than 30 or fewer than 10 cigarettes daily.

Earlier studies of Scandinavian twins reported a moderate genetic effect on smoking. But the new study "is much more sophisticated methodologically than previous research — and therefore stronger," maintains John R. Hughes of the University of Vermont in Burlington. The combined findings suggest that this effect is universal, he adds.

Also novel here are data from the same subjects at two different times. In fact, the 16 years between surveys spanned a period of growing social intolerance to smoking, notes Neal L. Benowitz of the University of California, San Francisco. Smoking prevalence nearly halved between surveys, he notes in an editorial accompanying the new report. That the second survey showed 27 percent of the men still smoked in the face of increasing pressure to quit — "reflects [their] more severe and persistent drug dependence," Benowitz says.

"It is notable," he adds, "that one of the strongest genetic effects was on light smoking." Indeed, he concludes, the new data suggest that "light and heavy smoking may be influenced by different genes." — *J. Raloff*