Some Number-Theoretic Calculations

K. E. Kloss

An account is given of several number-theoretic computations carried out by the author, some with ranges many times those of any previous published work. The calculations pertain to (1) long sequences of consecutive composite numbers, (2) Fermat quotients, (3) Wilson quotients, (4) generalized Wilson quotients, (5) Pell's equation, (6) the partition function, (7) a conjecture of Feit and Thompson, and (8) unique factorization quadratic domains.

Key words: Numbers, theory of, primes.

The purpose of this note is to enumerate some number-theoretic calculations carried out by the author in the past four years. By so doing, we hope to prevent needless repetition of the calculations elsewhere. We expect to describe most of the computations in greater detail in later articles; our intention here is just to offer a convenient summary. Most of the calculations were done on the NBS PILOT computer, a decimal and hexadecimal machine with a 65-bit word.

The results obtained were the following:

1. Consecutive Composite Numbers. The greatest difference between consecutive primes less than 128,000,000 is 222. It occurs between $p_0 = 122,164,747$ and $p_0 + 222$.

2. Fermat Quotients. For p an odd prime, the congruence

$$a^{p-1} \equiv 1 \qquad \mathrm{mod}\ p^2$$

is important in the "first case" of Fermat's Last Theorem, for it is known (J. B. Rosser, An additional criterion for the first case of Fermat's last theorem, Bull-AMS **47** (1941), 109–110) that a counterexample to the Theorem, with odd prime exponent p, can exist only if this congruence is satisfied by all primes $a \leqslant 43$. The following table gives, for all primes $a \leqslant 43$, all odd prime solutions p of the congruence which are less than the indicated range $R(a)$ of the calculation.

3. Wilson Quotients. The only known solutions of

$$(p-1)! + 1 \equiv 0 \ \mathrm{mod}\ p^2$$

are $p = 5$; 13; 563. There are no other solutions $p < 1,017,000$, but there are some "near" solutions like

$$\{(780,886)! + 1\}/780,887 \equiv -1 \qquad \mathrm{mod}\ 780,887.$$

TABLE 1. *Odd prime solutions of* $a^{p-1} \equiv 1\ mod\ p^2$

a	$R(a)$	p
2	31,059,000	1,093; 3,511
3	10,752,000	11; 1,006,003
5	5,250,000	20,771; 40,487
7	10,057,000	5; 491,531
11	7,736,000	71
13	5,243,500	7; 863; 1,747,591
17	5,415,900	3; 46,021; 48,947
19	5,583,900	3; 13; 43; 137
23	5,131,970	13; 2,481,757
29	10,431,000	No solutions found.
31	10,450,000	7; 79; 6,451
37	10,309,750	3; 77,867
41	9,500,000	29; 1,025,273
43	5,430,200	5; 103

4. Generalized Wilson Quotients. Let $t(n)$ denote the product of all positive integers less than and relatively prime to n. In the range $3 \leqslant n < 32,000$, the only n for which

$$t(n) \equiv \pm 1 \qquad \mathrm{mod}\ n^2$$

were found to be $n = 5$; 13; 563 (see sec. 3) and

$$n = 5,971 = 7 \times 853.$$

5. Pell's Equation. A table was prepared showing all integers $N < 96,562$ for which

$$x^2 - Ny^2 = -1 \tag{1}$$

has solutions in integers x, y. There is also a table of all integers $N < 96,562$ which are the sum of two relatively prime squares and for which (1) is not solvable.

6. Partition Function. Let $p(n)$ denote the number of (unrestricted) partitions of n. Tables of $p(n)$ mod m were calculated for $m = 11^7$ and 13^7 ($n \leqslant 25,000$), and $m = 19^6$, 23^5, 29^2 ($n \leqslant 1,000$).

In addition it was shown that for each prime q in the range $13 \le q \le 47$, and for every integer b, there is an integer $a > 0$ such that $p(aq+b) \not\equiv 0 \bmod q$.

7. *A Conjecture of Feit and Thompson.* There are no primes $p < 550{,}800$ such that

$p^2 + p + 1$ is a prime and $3^p \equiv 1 \bmod (p^2 + p + 1)$.

This is in agreement with the Feit-Thompson conjecture that

$$\left(\frac{p^q - 1}{p - 1}, \frac{q^p - 1}{q - 1} \right) = 1$$

for distinct primes p and q. The displayed condition is equivalent to the conjecture for the case $q = 3$.

8. *Unique Factorization Domains.* For primes $p \equiv 1 \bmod 4$, let $h(p)$ denote the class number of the integral domain

$$\left\{ \frac{a + b\sqrt{p}}{2} : a, b \text{ rational integers of the same parity} \right\}.$$

For $p < 120{,}000$, approximately 80 percent of such integral domains have unique factorization (i.e., have $h(p) = 1$). A table of such p yielded this information.

In addition, a table of $h(p)$ for $p < 95{,}000$ was calculated.