PI MU EPSILON JOURNAL

VOLUME 10 SPRING 1995 NUMBER 2

CONTENTS

(continued on inside back cover)

DIVISIBILITY TESTS FOR PRIMES GREATER THAN 5

Phil Plummer
Portland State University

Many papers have been written giving divisibility tests for integers. This note does not contain any new result, but it gathers previous tests in one place and shows how to generate any number of new ones.

Divisibility tests for 2, 3, 4, 5, 8, and 10 are taught as early as elementary school but tests for arbitrary prime numbers are not given. Here is a test for divisibility by 7. Take the number to be tested and double its last digit. Subtract this from the number with its last digit removed. If 7 divides this new number, then 7 divides the original. For example, $7 \mid 294$ since $7 \mid (29 - 2 \cdot 4) = 21$. Alternatively, one can multiply the last digit by 5 and add the result: $7 \mid 294$ since $7 \mid (29 + 5 \cdot 4) = 49$.

Consider the number 51, a multiple of 17. Does $17 \mid 51$ because $17 \mid (5 - 5 \cdot 1) = 0$? In other words, does 5 work for 17 the same way that 2 works for 7? The answer is "yes". The proof is as follows. Let $x = 10a + b$ and $r = a - 5b$. We have

$$x + 7r = (10a + b) + 7(a - 5b) = 17a - 34b.$$

If $17 \mid r$, then $17 \mid 7r$. Since $17 \mid (x + 7r)$ we have that $17 \mid x$.

By generalizing this procedure we can prove that a test can devised for any prime and we can find the constant ti. However, if we had a 50-digit number to be tested for divisibility by 7, removing only one digit at a time would be time-consuming indeed. But if we removed ten digits for each iteration it would cut the calculation time needed immensely. A test can be given where the number of digits removed at each stage, y, can be chosen arbitrarily:

THEOREM 1. Given a prime p and $x = 10^y a + b$, let $r = a + nb$ where n is the solution to $10^y n \equiv 1 \pmod p$. If $p \mid r$ then $p \mid x$.

Proof. Let n' be such that $nn' \equiv 1 \pmod p$. Note that $10^y nn' \equiv n' \pmod p$ so $10^y \equiv n' \pmod p$. Thus, both $10^y - n'$ and $1 - nn'$ are $\equiv 0 \pmod p$. We have

$$x + n'r = 10^y a + b + n'(a - nb)$$
$$= (10^y - n')a + b(1 - nn') \equiv 0 + 0 \pmod p.$$

If $p \mid r$, then $p \mid n'r$. Since $p \mid x + n'r$ we have that $p \mid x$.

In exactly the same way we could prove

THEOREM 2. Given a prime p and $x = 10^y a + b$, let $r = a - mb$, where m is the solution to $10^y m \equiv -1 \pmod p$. If $p \mid r$ then $p \mid x$.

There is a connection between m and n.

COROLLARY. $m = p - n$.

Proof. Since $10^y n \equiv 1 \pmod p$ and $10^y m \equiv -1 \pmod p$, we have $10^y (n + m) \equiv 0 \pmod p$, and so $n + m \equiv 0 \pmod p$. Since m and n are both between 0 and p, the corollary follows.

For an example, let us take $x = 28{,}842$, $p = 23$, and $y = 2$. To determine n we solve $10^2 n \equiv 1 \pmod{23}$. This is $8n \equiv 1 \pmod{23}$, so $n = 3$. Thus, $23 \mid 28{,}842$ if $23 \mid (288 + 3 \cdot 42) = 414$. Does $23 \mid 414$? It will if $23 \mid (4 + 3 \cdot 14) = 46$. Since it does, it follows that $23 \mid 28{,}842$.

The table on the next page gives, for primes $p < 100$, the value of n for $y = 1, 2, \ldots, 12$. The values of n are periodic, with period equal to the order of 10 (mod p).

If we let n_y denote the value of n for y, then we have

THEOREM 3. $n_{y+1} \equiv n_1 n_y \pmod p$.

Proof. $10^{y+1} n_{y+1} \equiv 1 \equiv 1 \cdot 1 \equiv (10 n_1)(10^y n_y) \pmod p$.

This recursive property allows the generation of large tables very quickly in a spreadsheet program without the problem of roundoff error. For efficient tests, small values of n (or $m = p - n$) can be quickly determined.

Phil Plummer received his B. S. degree in mathematics and physics at Portland State University and is currently finishing work toward his M. S. degree in mathematics. He wishes to thank his high-school mathematics teacher, Mr. Wayne Wheeler of Springfield (Oregon) High School, for teaching him that mathematics could be fun.

y (number of digits removed)

	1	2	3	4	5	6	7	8	9	10	11	12
3	1	1	1	1	1	1	1	1	1	1	1	1
7	5	4	6	2	3	1	5	4	6	2	3	1
11	10	1	10	1	10	1	10	1	10	1	10	1
13	4	3	12	9	10	1	4	3	12	9	10	1
17	12	8	11	13	3	2	7	16	5	9	6	4
19	2	4	8	16	13	7	14	9	18	17	15	11
23	7	3	21	9	17	4	5	12	15	13	22	16
29	3	9	27	23	11	4	12	7	21	5	15	16
31	28	9	4	19	5	16	14	20	2	25	18	8
37	26	10	1	26	10	1	26	10	1	26	10	1
41	37	16	18	10	1	37	16	18	10	1	37	16
43	13	40	4	9	31	16	36	38	21	15	23	41
47	33	8	29	17	44	42	23	7	43	9	15	25
53	16	44	15	28	24	13	49	42	36	46	47	10
59	6	36	39	57	47	46	40	4	24	26	38	51
61	55	36	28	15	32	52	54	42	53	48	17	20
67	47	65	40	4	54	59	26	16	15	35	37	64
71	64	49	12	58	20	2	57	27	24	45	40	4
73	22	46	63	72	51	27	10	1	22	46	63	72
79	8	64	38	67	62	22	18	65	46	52	21	10
83	25	44	21	27	11	26	69	65	48	38	37	12
89	9	81	17	64	42	22	20	22	18	73	34	39
97	68	65	55	54	83	18	60	6	20	2	39	33

n (multiplier for the last y digits)

A PROOF OF PASCAL'S HEXAGON THEOREM USING ABRIDGED NOTATION

Margaret Maxfield
Louisiana Tech University

In a recent article about Pascal's hexagon theorem for a circle, Jan van Yzeren [2] credited H. Guggenheimer with a previous **proof.** However, Professor Guggenheimer [1] explained that the proof had in fact been taught him in his 11th grade Descriptive Geometry class in **Basel,** Switzerland. The following proof, which I learned as a college junior, used to be called a proof by "abridged notation". In it, a linear form is represented by a single letter, and forms are combined to make second-degree expressions that will stand for conic sections.

For example, if $\alpha = x + 2y + 1$ and $\beta = x - 2y + 2$, then $\alpha = 0$ and $\beta = 1$ are equations of lines, $\alpha\beta = 0$ is the equation of a pair of intersecting lines (a degenerate conic—asymptotes only), and $\alpha\beta = 1$ is the equation of a nondegenerate hyperbola.

Any equation of the form $\alpha + k\beta = 0$ represents a line (it is linear in form) that passes through the intersection of the lines $\alpha = 0$ and $\beta = 0$ since substitution of the coordinates of the point of intersection make both α and β take on the value 0. We use a similar strategy for conic sections. If $S = 0$ and $T = 0$ are conies, then they are of second degree in x and y. Then for any nonzero constant k, $S + kT = 0$ is of second degree so it represents a conic. Since the point where S and T intersect has coordinates that satisfy both $S = 0$ and $T = 0$, the conic $S + kT = 0$ passes through the points of intersection.

PASCAL'S THEOREM: If a closed hexagon is inscribed in a conic section, then the three points of intersection of its opposite sides are collinear.

(If the two opposite sides are parallel, their point of intersection is taken to be the point at infinity. The conic section may be degenerate, and the