

## DIGIT-BASED FACTORING TRICKS

STUART M. ANDERSON

ABSTRACT. There are several specialized tricks for determining whether an integer is divisible by small divisors. We will look at where these tricks come from, and set up a general method for finding all these tricks for any divisor.

Since most factoring tricks involve manipulating the digits of numbers, they are connected to patterns in the digits. Therefore, let's start with the idea of a repeating decimal. As everyone knows, if a number is rational, it will be expressed as a decimal that repeats a pattern of digits forever. However, there are other, more hidden patterns in the decimal form of a rational number, and it is these other patterns that produce many of the factoring tricks. To find these other patterns, we will find the equation that describes the repeating decimal pattern, and then make a generalization of it, which will give the other patterns.

For example, let  $p = 7$ , so the decimal expression for  $\frac{1}{7}$  is  $0.142857142857\dots$ . Then if we define  $q = 142857$ , the decimal can be written as

$$\frac{q}{10^6} + \frac{q}{10^{12}} + \dots = \frac{q}{10^6} \sum_0^{\infty} (10^{-6})^n .$$

Now since this kind of sum has the solution  $\sum_0^{\infty} a^n = \frac{1}{1-a}$ , we get the result that

$$\frac{1}{7} = \frac{q}{10^6} \frac{1}{1-10^{-6}}$$

. Therefore, if we rearrange and simplify this equation, we get  $10^6 = 7q + 1$ . This shows that the numbers  $q$  and 1 are just the quotient and remainder when  $10^6$  is divided by 7.

What happens if we try to generalize this, and look at equations like  $b^s = pq + r$ ? In this case,  $b$  is the base (which is usually 10),  $s$  is the size of the repeating group of digits,  $p$  is the divisor,  $q$  is the quotient, and  $r$  is the remainder. Now if we reverse the process we just did, we can get an infinite sum that shows a new digit pattern. Solving the equation gives

$$\frac{1}{p} = \frac{q}{b^s - r} = \frac{q}{b^s} \frac{1}{1 - rb^{-s}} = \frac{q}{b^s} \sum_0^{\infty} \left(\frac{r}{b^s}\right)^n .$$

For any choices of  $p, b, s$ , this infinite sum shows a pattern in the digits of the base- $b$  expansion, namely that a group of digits of size  $s$  is repeated, but multiplied by  $r$  each time it is repeated. Because this causes the group of digits to grow, the size of the group will not remain  $s$ , and the extra digits will be carried into the next group to the left. This obscures the pattern except in the special case when  $r = 1$ , which (when  $b = 10$ ) gives the usual repeating decimal we all know.

---

*Date:* January 16, 2006.

For  $b = 10$ ,  $p = 7$ , and various choices of  $s$  we get

$$\begin{array}{llll}
 s = 1 & q = 1 & r = 3 & \frac{1}{7} = \frac{1}{10} \sum_0^{\infty} \left( \frac{3}{10^1} \right)^n \\
 s = 2 & q = 14 & r = 2 & \frac{1}{7} = \frac{14}{100} \sum_0^{\infty} \left( \frac{2}{10^2} \right)^n \\
 s = 3 & q = 142 & r = 6 & \frac{1}{7} = \frac{142}{1000} \sum_0^{\infty} \left( \frac{6}{10^3} \right)^n \\
 s = 4 & q = 1428 & r = 4 & \frac{1}{7} = \frac{1428}{10000} \sum_0^{\infty} \left( \frac{4}{10^4} \right)^n \\
 s = 5 & q = 14285 & r = 5 & \frac{1}{7} = \frac{14285}{100000} \sum_0^{\infty} \left( \frac{5}{10^5} \right)^n \\
 s = 6 & q = 142857 & r = 1 & \frac{1}{7} = \frac{142857}{1000000} \sum_0^{\infty} \left( \frac{1}{10^6} \right)^n .
 \end{array}$$

Notice that  $q$  just keeps appending the digits of the normal decimal pattern, while  $r$  passes through the sequence 3, 2, 6, 4, 5, 1. The values for  $r$  are easier to compute than one would think at first, because each one leads simply to the next. The reason for this is easy to see from an example: Since  $10^3 = 7 \times 142 + 6$ , then  $10^4 = 7 \times 1420 + 60$ . Since the first term is already a multiple of 7, the remainder must come from the last term only. Thus  $60 = 7 \times 8 + 4$ , so the next  $q$  is 4. Therefore, to get the next value of  $q$ , multiply the previous  $q$  by 10, then take the remainder of division by 7 as the next  $q$ . In general, the same rule works: if you know the value of  $r$  for a particular choice of  $b, p, s$ , then to get the  $r$  for  $b, p, s + 1$ , you take the old  $r$  and compute the remainder of  $br/p$  to get the next  $r$ .

This is an example of modular arithmetic, in which the result of every calculation is replaced by its remainder when divided by the modulus. In our example the modulus is 7, but it could be any positive integer. Modular arithmetic works just like ordinary arithmetic, in the sense that one can add, subtract, multiply, divide, take reciprocals, etc. and always get an answer that is consistent and makes sense within the context of modular arithmetic.

For example, in modulo 7 arithmetic, the only numbers are 0, 1, 2, 3, 4, 5, 6 because anything larger gets reduced down to its remainder by division by 7. Then  $3 \times 4 = 12 \equiv 5 \pmod{7}$ , where the “ $\equiv$ ” sign means “these have the same remainder when divided by the modulus,” and “mod 7” is just a reminder that the modulus is 7. But then since  $3 \times 4 \equiv 5 \pmod{7}$ , it must be true that  $5/3 \equiv 4 \pmod{7}$ . This looks strange, but it really means that whenever a number with remainder 3 divides evenly into a number with remainder 5, then the answer will be a number with remainder 4.

There are many theorems known about modular arithmetic, most of which are easy to prove by simple calculations. The most important for us is that for any positive integers  $b, p$ , the pattern of  $r$  values eventually starts to repeat. This is obvious, because there are only a finite number of possible remainders when we divide by  $p$ , namely the values  $0, 1, \dots, p - 1$ , so the sequence must eventually reuse one of them. But because we get the next  $r$  from the previous one, the pattern

must repeat after this point. This first theorem, by the way, is how we prove that every fraction has a repeating decimal expression.

There are two special cases of this theorem, as well: first, if there is an  $s$  so that  $p$  divides evenly into  $b^s$ , then for this value of  $s$ , we must get  $r = 0$ , and as soon as that happens, all the  $r$  values after that point will also be 0. This happens, for example, when  $p = 4, b = 10$ , because 4 divides evenly into  $10^2$ ; it is easy to check that  $r = 0$  whenever  $s \geq 2$ . Second, if  $p$  and  $b$  have no common factor, then there is an exponent  $s > 0$  so that  $b^s \equiv 1 \pmod{p}$ ; in other words, our pattern of values of  $r$  will always eventually get to a power of  $b$  where  $r = 1$ .

The other theorem is that, for any modulus  $p$ , the value  $p - x$  acts just like  $-x$  in modular arithmetic. This means that, for example, when  $b = 10, p = 7, r = 6$ , we could have also used  $r = -1$  in any trick based on  $r = 6$ , because  $6 = 7 - 1 \equiv -1 \pmod{7}$ .

We now have two ways to derive factoring tricks, one based on the infinite sum, and one based on the corresponding equation. They are equivalent, but one way may be clearer than the other. We will start with the equation. If we write the equation  $b^s = pq + r$  using modular arithmetic, it says  $b^s \equiv r \pmod{p}$ . This means that we can replace  $b^s$  with  $r$  in any arithmetic calculation, and the answer will be equivalent modulo  $p$  to the original answer. Therefore we can take *any* group of digits (as long as they are at least  $s$  places to the left of the decimal point), shift them  $s$  places to the right, multiply by  $r$ , and add them to the remaining digits.

The best choice is usually to take a group of size  $s$ ; a smaller group will not shorten  $n$  very much, and a larger group will waste the effort of calculating more digits, but will still not shorten  $n$  any more than  $s$  digits. Therefore, for any positive integer, we should group its digits into groups of size  $s$  and write the number using a “base  $b^s$ ” notation, and then apply our equation to simplify it. The calculation looks like this using the example of  $p = 7, s = 2, r = 2, n = 1234567890$ :

$$\begin{aligned} n &= (((12 \times 10^2 + 34) \times 10^2 + 56) \times 10^2 + 78) \times 10^2 + 90 \\ &\equiv (((12 \times 2 + 34) \times 2 + 56) \times 2 + 78) \times 2 + 90 \pmod{7} \\ &= 934 = 9 \times 10^2 + 34 \\ &\equiv 9 \times 2 + 34 \pmod{7} \\ &= 52 \\ &\equiv 3 \pmod{7} \end{aligned}$$

Therefore 1234567890 has remainder 3 when divided by 7. Looking at the calculation, we can see that the process can be described in words easily:

**Rule 1.** *Using the equation  $b^s = pq + r$ , group the digits of  $n$  in sets of size  $s$  starting from the right; then, starting from the left, multiply each group by  $r$ , shift it to the right to line up with the next group, and add it to the next group. Repeat until the number is only  $s$  digits long or less. This new value is  $n'$ , and satisfies  $n' \equiv n \pmod{p}$ .*

What does this same trick look like when we start with the series instead of the equation? The corresponding series is

$$\frac{1}{p} = \frac{q}{b^s} \sum_0^{\infty} \left(\frac{r}{b^s}\right)^n .$$

Once again, let's group the digits of  $n$  into groups of size  $s = 2$ , writing it a little differently this time:  $n = 12 \times (10^2)^4 + 34 \times (10^2)^3 + 56 \times (10^2)^2 + 78 \times (10^2)^1 + 90 \times (10^2)^0$ . Now all the groups of digits except the very last one have at least one factor of  $10^2$  multiplying them. Look at the first group of digits, divide it by 7 using our sum formula, and observe what happens if we follow the rule that we should shift it  $c$  places to the right and multiply it by  $r$ :

$$\begin{aligned} \frac{12 \times 10^8}{7} &= 12 \times 10^8 \times \frac{14}{100} \sum_0^{\infty} \left( \frac{2}{10^2} \right)^n \\ &= 168 \times (10^6 + 2 \times 10^4 + 4 \times 10^2 + 8 + 16 \times 10^{-2} + 32 \times 10^{-4} + \dots) \\ \frac{12 \times 10^6 \times 2}{7} &= 12 \times 10^6 \times \frac{14}{100} \sum_0^{\infty} 2 \times \left( \frac{2}{10^2} \right)^n \\ &= 168 \times (2 \times 10^4 + 4 \times 10^2 + 8 + 16 \times 10^{-2} + 32 \times 10^{-4} + \dots) \end{aligned}$$

Shifting the digits two places to the right is the same as dividing by 100, which reduces all the exponents by 2, while doubling puts the extra factor of 2 in the sum. The important thing to notice here is that the terms in the sum with positive powers of 10 must be integers, and the terms with negative powers of 10 give the fractional part of the number. But while the integer part changed, the fractional part did not. This is because multiplying by 2 and dividing by  $10^2$  shifts every term in the sum one step to the right, and so one term is moved from the integer part to the fractional part. Therefore the integer part of the sum gets shorter, but since the fractional part of the sum has an infinite number of terms already, shifting each term one step to the right does not change it at all. But the fractional part is what tells us the remainder, so the remainder doesn't change when we do this. This is the reason why our rule works, when we look at it from the point of view of the infinite sum instead of the equation.

We have used the example of division by 7 here because it is easier to show how it works with a concrete example, but the method would work for any number, even numbers that are not prime. We will stick to primes, though, because that is all we really need. If we are lucky, as with 3 and 11, the repeating decimal will be short, and we get a very good rule, while with numbers like 7 and 13, the repeating decimal unit is longer, and it is more difficult to find a good rule. However if we keep trying out larger and larger values of  $s$ , we must eventually find a case where  $b^s \equiv 1 \pmod{p}$  or  $b^s \equiv 0 \pmod{p}$ . The first case gives a repeating decimal, and the second case gives a terminating decimal.

Now for any number  $p$ , there are actually an infinite number of factoring tricks, but most of them are not useful. The best ones are those which involve the smallest groups of digits (i.e., the smallest  $s$ ) and which have the simplest  $r$ . The best possible value is  $r = 0$ , because then our rule says to multiply each group by 0 and add it to the next group, which is just the same as saying that we simply ignore all groups except the one furthest to the right. This is obviously the simplest trick of all. The next best trick is found from  $r = 1$ , where we simply add each group to the next one on its right. After this, the third best rule is found from  $r = p - 1$ , where we treat  $p - 1$  as  $-1$  and subtract each group from the next one on its right. After that, of course come rules based on 2 and  $p - 2$ , and so on.

It is also better to have a smaller value for  $s$  because the number of digits you add when applying a rule is always about the same as the number of digits of  $n$  (actually a little bit more because of carrying digits), but with a smaller  $s$ , you end up with a shorter number. So for example, if the best  $q$  has a really large  $s$  but the second best  $q$  has a much smaller  $s$ , it may be quicker and more efficient to use the second best  $q$ .

We can also mix rules. For example,  $b = 10, s = 6, p = 7$  gives an  $r = 1$  rule with a digit group size of 6, and we can use this easy rule to reduce a huge number down to at most 6 digits. Then  $b = 10, s = 3, p = 7$  gives an  $r = 6 \equiv -1 \pmod{7}$  rule with a group size of 3 digits, which we can use to reduce the number down to at most 3 digits. Then  $b = 10, s = 2, p = 7$  gives an  $r = 2$  rule that reduces the number down to at most 2 digits. Finally,  $b = 10, s = 1, p = 7$  gives an  $r = 3$  rule that reduces the number down to a single digit. The calculation looks like this for our previous example,  $n = 1234567890$ :

$$\begin{aligned} n &= 1234567890 \\ &\equiv 1234 \times 1 + 567890 = 569124 \pmod{7} \\ &\equiv 569 \times -1 + 124 = -445 \pmod{7} \\ &\equiv -4 \times 2 + -45 = -53 \pmod{7} \\ &\equiv -5 \times 3 - 3 = -18 \equiv -1 \times 3 - 8 = -11 \equiv -1 \times 3 - 1 = -4 \equiv 3 \pmod{7} \end{aligned}$$

As you can see, we applied the  $r = 1$  rule once,  $r = -1$  once,  $r = 2$  once, and  $r = 3$  three times. We were forced to use worse  $q$  values as we went along, because we needed smaller  $s$  values to keep reducing the size of  $n$ . The  $q = 3$  part wasn't strictly necessary, because once we reached the number  $-53$  it was easy to divide by 7 directly. We did it to show the disadvantage of rules with larger values of  $r$ , which is that they don't shorten the number very fast because they keep carrying digits back to the left.

Now that we have a rule for automatically generating factoring tricks, let's go down the list of prime numbers and watch how it works (see Table 1). We will use  $b = 10$  to stay in the standard decimal notation, but of course, we could also generate tricks for binary, hexadecimal, octal, or in fact any number base.

Now that we have this large table of values, what are the best rules? For 2 and 5, we get  $r = 0$  when  $s = 1$ , so we should simply delete all digits except the last one. For 3, we get  $r = 1$  when  $s = 1$ , so we should add each single digit to its neighbor. For 7 have many choices, but the best are to add each group of size 6 to its next neighbor, or subtract each group of 3 from its next neighbor, or double each group of 2 and add it to its next neighbor. For 11, we can either add each pair of digits to its neighbor, or subtract each single digit from its neighbor. For 13, the rules are the same as the first two rules for 7, but the third rule for 7 does not work because we get  $r = 9$  when  $s = 2$ . We can use a trick to get a fairly good rule from this, however, if we notice that  $9 = 10 - 1$ , so that shifting a pair of digits two places to the right and multiplying by 9 is the same as shifting the pair one place to the right and adding, then one more place to the right and subtracting.

In the first column of our table, we were very lucky: 2 and 5 divide into 10, so we get very simple rules for them, while 3, 11, and 13 all have rules that reach  $r = 1$  for small values of  $s$ . In general, for a prime number  $p$ , the value of  $s$  where  $q = 1$  could be up to  $p - 1$ , and we see that this is the case for  $p = 7$ . This is why the rules for 7 are not as good or as easy to find as for 2, 3, 5, 11. With 13 we are

p	s	r	p	s	r	p	s	r	p	s	r	p	s	r
2	1	0	17	1	10	19	1	10	23	1	10	23	18	9
3	1	1		2	15		2	5		2	8		19	21
5	1	0		3	14		3	12		3	11		20	3
7	1	3		4	4		4	6		4	18		21	7
	2	2		5	6		5	3		5	19		22	1
	3	6		6	9		6	11		6	6	29	1	10
	4	4		7	5		7	15		7	14		2	13
	5	5		8	16		8	17		8	2		3	14
	6	1		9	7		9	18		9	20		4	24
11	1	10		10	2		10	9		10	16		5	8
	2	1		11	3		11	14		11	22		6	22
13	1	10		12	13		12	7		12	13		7	17
	2	9		13	11		13	13		13	15		8	25
	3	12		14	8		14	16		14	12		9	18
	4	3		15	12		15	8		15	5		10	6
	5	4		16	1		16	4		16	4		11	2
	6	1					17	2		17	17		12	20
							18	1						

TABLE 1. Table 1:  $s$  and  $r(s)$  for primes  $p < 30$ .

still lucky, because we might have had to go as high as  $s = 12$ , but we actually find  $q = 1$  at  $s = 6$ . After 13, however, our luck runs out. All of the remaining prime numbers have  $q = 1$  when  $s = p - 1$ , the worst possible case.

We can still find rules for these prime numbers, but the rules are not as good. For  $p = 17, 19, 23, 29$ , we can add groups of size  $p - 1$  to their next neighbor, or subtract groups of size  $(p - 1)/2$  from their next neighbor, which does let us reduce huge numbers down to ones with at most  $(p - 1)/2$  digits. These are still large numbers, so the rules are not very strong. For 17, we get  $r = 15 \equiv -2 \pmod{17}$  when  $s = 2$ , so we can take a pair of digits, double it and subtract it from its neighbor. This is very good, because it reduces our number to at most 2 digits. For 19 we get  $r = 12$  when  $s = 3$ , so we can take each group of 3 digits, shift it 2 places to the right and add, then shift it one more place to the right, double it, and add. This is a messy rule, but it will reduce a number to 3 digits. For 23, we get  $r = 11$  when  $s = 3$ , so we can use the same rule as for  $p = 19$ , except that we omit the doubling. For 29, we find  $r = 2$  when  $s = 11$ , so we can take a group of 11 digits, double it, and add it to its next neighbor. We could also use the fact that  $r = 22$  when  $s = 6$  to take a group of 6 digits, double it, shift it 5 places and also 6 places to the right, and add. We could also use  $r = 13$  when  $s = 2$  to shift a pair of digits one place to the right, add, then shift it one more place, triple it, and add. This would reduce the number to 2 digits, but is a complicated rule.

There is one final point to note about the rules that we find in our table: once  $p > 10$ , the first value of  $r$  is always 10, which gives the useless rule that we should take a single digit, shift it one place to the right, multiply it by 10, and add. But multiplying by 10 simply shifts the digit one place to the left, putting it back where it started. Therefore the rule is true, in the sense that it doesn't change the remainder mod  $p$ , but useless, because it returns the original  $n$  unchanged. For

large values of  $p$ , there will be more of these useless rules: if  $p > 10^k$  then the first few values of  $r$  will be  $10^s$  when  $s \leq k$ . There will also be redundant rules. For example, when  $p = 23, s = 8$  and when  $p = 29, s = 11$  we get  $r = 2$ . But on the next line of the table, we get  $r = 20$ , because of course we get the next  $r$  by multiplying the previous  $r$  by 10 and taking the remainder mod  $p$ . Since  $20 < p$  in both cases, the remainder is just 20. But this means that the rule we get from this line of the table is exactly the same as the rule from the previous line. This is because we are shifting one more place to the right, but then multiplying by an extra factor of 10, which shifts the digits back one place to the left again.

This brings up one final consideration: when  $r$  is two or more digits long, we are shifting a group of length  $s$  to the right by  $s$  places, then shifting back one or more places. Therefore, it is better to use a smaller group of digits, since we cannot reduce the length of  $n$  by  $s$  digits any more. The best group size to use is  $s - d$ , where  $d$  is the number of digits of  $r$ .

Summary: For any number base  $b$  and prime number  $p$ , let  $b^s = p \times q(s) + r(s)$ , where  $q(s)$  and  $r(s)$  are the quotient and remainder, and are functions of  $s$ . We can find  $r(s)$  from the rule that  $r(0) = 1$  and  $r(s + 1) \equiv b \times r(s) \pmod{p}$ . Then for any integer  $n$ , we can take any group of digits that are at least  $s$  places to the left of the decimal, shift them  $s$  places to the right, multiply them by  $r(s)$ , and add them to the remaining digits, and this will not change the remainder when  $n$  is divided by  $p$ . The best rules are those where  $s$  is small and  $q(s) \equiv 0, \pm 1 \pmod{p}$ , and the best digit group size to use is  $s - d$ , where  $d$  is the length of  $r$ .