FUN WITH NUMBERS

THOMAS S. SHORES

Who knew powers of 2 were so powerful ...

Here's a fun fact: Write down the nine digits of your SSN: Then you can be absolutely certain that there is some power of 2, say 2^N for some natural number (positive integer) N, whose first nine digits are exactly your SSN. For example, if your SSN is 214-74-8364, then 2^{31} works like a charm. Check it on your calculator. Surprising, right? This little essay will demonstrate why this is so with a complete justification by way of some rigorous mathematics. I'll have to assume that the reader has some memory of high school algebra and geometry. I'll also assume a knowledge of the very basic axiomatic properties of arithmetic. Subject to those restrictions, I'll try to make this essay as self-contained as possible. Consequently, I'll have to give a very modest introduction to number theory. Just for the record: *number theory* is that ancient branch of mathematics that studies the properties of natural numbers and whatever that entails (and over the centuries, that has entailed a whole lot!). This introduction will also include some number theory that really isn't necessary for explaining the "powers of 2" problem – it's just there for fun.

Ok, first a acknowledgement: The inspiration for this essay comes from one of the "Great Courses" offerings, the elegant "Introduction to Number Theory" by Professor Edward B. Burger. In particular, he made the "powers of 2" claim in Lecture 2 as a bit of a teaser for what was to come in later lectures. I hope that this essay will be of particular interest to anyone who watched "Introduction to Number Theory."

Note. To non-specialists: As I indicated above, this will be an elementary introduction to number theory. "Elementary" doesn't necessarily mean easy: You'll have think carefully about some of the details that I offer in this essay. But it does mean that I assume no greater background than the mathematics that you receive in high school algebra and geometry. Additionally, there are a few exercises at the end of this essay so that you can flex your number theory muscles on them.

Note. To specialists: You may find most of this essay excruciatingly boring, so just yawn yourself through those parts and I hope that you find an item or two of interest along the way.

Numbers and More Numbers

Let's begin our adventure by placing some of the number notation I'll use up front. Refer back to this if you run into forgotten terminology as you read the essay:

- The *natural numbers* are the numbers in the infinite sequence $1, 2, 3, \ldots$.
- The *integers* are the whole numbers $0, \pm 1, \pm 2, \pm 3, \ldots$.
- The integer p is said to *divide the integer q (evenly)* or is said to be a *factor* of q if there exists another integer m such that $q = m \cdot p$. In this case we'll write $p \,|\, q$. We'll usually drop the '$\cdot$' and write the product as $q = mp$ unless there is a possibility of confusion.
- A *prime number* p is a natural number greater than 1 that cannot be factored into a product of natural numbers other than with factors 1 and p.
- The *greatest common divisor* of two integers a and b, not both 0, is the largest natural number d such $d \,|\, a$ and $d \,|\, b$. In this case we write $d = \gcd\{a, b\}$.
- Two integers a and b are *relatively prime* if $\gcd\{a, b\} = 1$.
- Given integers a and b along with integers m and n, the expression $ma+nb$ is called a *linear combination* of a and b.
- The *rational numbers* are those of the form p/q with p, q integers, $q \neq 0$.
- The *real numbers* are numbers that correspond to points on a number line or, equivalently, numbers that can be represented by a possibly infinite decimal expansion.
- The real number α is called *algebraic of degree d* if it is a solution to some polynomial equation with integer coefficients of degree d in the variable x and *transcendental* if it does not satisfy any such equation.
- The *interval* $[0, 1]$ consists of all real numbers α satisfying $0 \leq \alpha \leq 1$.
- Given a real number α, the *absolute value* of α is the nonnegative number $|\alpha|$ which is α if $\alpha \geq 0$ and $-\alpha$ otherwise. Geometrically, $|\alpha|$ is the distance between α and the origin on a number line.
- Given a real number α, $\lfloor \alpha \rfloor$ is the *integer part* of α, that is, the largest integer less than or equal to α and $\{\alpha\} = \alpha - \lfloor \alpha \rfloor$ is the *fractional part* of α. (In computer science, $\lfloor \alpha \rfloor$ is sometimes called the *floor* of α.)

- A set of numbers B is *dense* in a set of numbers A if, for any number α in A and arbitrary positive number ϵ, no matter how small, we can find a number β in B such that $|\alpha - \beta| < \epsilon$.

More colloqually, if we write a positive number α in decimal format, then $\lfloor \alpha \rfloor$ is the integer to the left of the decimal sign and $\{\alpha\}$ is the left over stuff to the right of the decimal sign. For example, $\sqrt{2} = 1.414213562\ldots$, so $\lfloor \sqrt{2} \rfloor = 1$ and $\{\sqrt{2}\} = 0.414213562\ldots$. It's a bit trickier for negative numbers: $\lfloor -\sqrt{2} \rfloor = -2$ and $\{\sqrt{2}\} = -\sqrt{2} - (-2) = 0.585786437\ldots$. Note that for any real number α we always have that $\{\alpha\}$ is in the interval $[0, 1]$, that is, $0 \leq \{\alpha\} \leq 1$.

Just for the record: $\sqrt{2}$ is probably the most famous irrational since it seems to be the first such number discovered (around the fifth century BCE) and in fact is reputed to have cost the Pythagorean Hipassus his life for exposing such an impiety. (So number theory may be more dangerous than you think!) Also, $x = \sqrt{2}$ is algebraic of degree 2 since it solves the equation $x^2 - 2 = 0$. And of course, any rational number p/q is algebraic of degree 1 since it solves the linear equation $qx - p = 0$. Thus, the algebraic numbers sit between the rational numbers and the reals.

Let's start at the beginning with a discussion of some of the fundamental properties of integers that go all the way back to Euclid and beyond. Here's a fact that we learned in grade school (ok, probably not the negative numbers), when we were first introduced to division. Its proof is actually a how-to-do-it prescription:

Theorem 1. *(Division algorithm) Given integers a and $b \neq 0$, there exists integers q and r such that $a = qb + r$ and $0 \leq r < |b|$.*

Proof. Let's first prove it for integer $a \geq 0$ and b. If $a < |b|$, we simply take $q = 0$ and $r = a$. Otherwise, subtract $|b|$ from a repeatedly for a total of q times until the difference $a - q\,|b| = r \geq 0$ is the smallest nonnegative integer possible. This is possible because the number of nonnegative integers less than a is finite, so we can't subtract $|b|$'s forever. Then r must be less than $|b|$ or we could subtract another $|b|$. Hence, we end up with $a = q\,|b| + r$. If $b > 0$, $b = |b|$ and we are done. If not, $-b = |b|$, so replace $|b|$ by b and q by $-q$ to obtain that $a = (-q)b + r$, which is what we want so we are done again. Next, if $a < 0$, by what we have just done we have $|a| = qb + r$, for integers q and $0 \leq r < |b|$. So if $r = 0$, we have $a = -\,|a| = -qb = (-q)b$ and we're done. Otherwise, if $b > 0$, we have

$$a = -\,|a| = -qb - r = -qb - b + b - r = (-q - 1)b + (b - r).$$

Now $b > b - r \geq 0$, so we're done again. We leave the last case of both $a < 0$ and $b < 0$ as an exercise. □

Remark. Just as a reminder, recall that in the Division Algorithm the number a is called the *dividend*, b the *divisor*, q the *quotient* and r the *remainder*.

Example 1. Apply the Division Algorithm to $a = 24987$ and $b = 314$ and identify terms.

Solution. For starters, 24987 is the dividend and 314 is the divisor. OK, I'm lazy and not going to do it the old grade school long division way. My ALAMA calculator says $a/b = 79.5796$ and $a - 79 \cdot b = 182$. So we obtain $a = qb + r$ with $q = 79$ as the quotient and $r = 182$ as the remainder. □

Next, we consider a really important extension of the Division Algorithm:

Euclidean Algorithm: Let a and $b \neq 0$ be integers. Apply the Division Algorithm repeatedly to the divisor/remainder pairs until we reach a remainder of 0 to obtain the sequence of divisions:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ &\vdots \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

Remark. Count r_0 as $|b|$. Thus, we have that $r_0 > r_1 > r_2 > \cdots > r_n \neq 0$. There has to be a final nonzero remainder since these numbers are all positive, so the last division yielding zero is justified. This algorithm has some important implications:

Theorem 2. *If the Euclidean Algorithm is applied to the integers a and b to yield a final positive remainder $d = r_n$, then d is the greatest common divisor of a and b.*

Proof. According to the last equation in the Euclidean Algorithm above, r_n is a divisor of r_{n-1}. But then we see that r_n is also a divisor of r_{n-2}, since it divides both terms of preceding equation $r_{n-2} = q_n r_{n-1} + r_n$, and can therefore be factored out. Next, we see that r_n is a divisor of both terms of the right-hand side of the equation $r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$ and again can be factored out, so that it is a divisor of r_{n-3}. Continuing in this fashion, we can work our way back to the third and second equations in the list to see that it is a divisor of r_0 and

b. Finally, the first equation shows that it is also a divisor of a. Hence, r_{n+1} is a common divisor of a and b.

Next, work our way forward in the equations: Suppose that the natural number d is a common divisor of a and b. Solve for r_1 in the first equation and we see that d is a factor in $a - q_1 b = r_1$, so it also divides r_1. Similarly, the second equation tells us that, since d divides both b and r_1, it also divides r_2. We can continue in this fashion all the way down to the last equation and deduce that d is a divisor of r_n. It follows that $d \leq r_n$, which shows that r_n is the *greatest* common divisor of a and b, i.e., we may write $r_n = \gcd\{a, b\}$. □

Example 2. Apply the Euclidean Algorithm to find $\gcd\{4578, 30072\}$.

Solution. Start with $a = 30072$ and $b = 4578$. We obtain this sequence of divisions:

$$\begin{aligned} 30072 &= 6 \cdot 4578 + 2604 \\ 4578 &= 1 \cdot 2604 + 1974 \\ 2604 &= 1 \cdot 1974 + 630 \\ 1974 &= 3 \cdot 630 + 84 \\ 630 &= 7 \cdot 84 + 42 \\ 84 &= 2 \cdot 42 + 0. \end{aligned}$$

Thus, we conclude that $\gcd\{4578, 30072\} = 42$. □

A few important consequences of the Euclidean Algorithm:

Theorem 3. *(Bézout's Identity) Let a and $b \neq 0$ be integers and $d = \gcd\{a, b\}$. Then d can be expressed as a linear combination of a and b, that is, there exist integers m and n such that $d = ma + nb$.*

Proof. We leave the case $r_1 = 0$ in the Euclidean algorithm as an exercise. Let's rewrite the statement of the Euclidean Algorithm by using each equation except the last one to solve for a remainder. It looks like this:

$$\begin{aligned} a - q_1 b &= r_1 \\ b - q_2 r_1 &= r_2 \\ r_1 - q_3 r_2 &= r_3 \\ r_2 - q_r r_3 &= r_4 \\ &\vdots \\ r_{n-3} - q_{n-1} r_{n-2} &= r_{n-1} \\ r_{n-2} - q_n r_{n-1} &= r_n \end{aligned}$$

From this we see that the first equation defines r_1 as a linear combination of a and b. If there is a second equation, we can substitute the first equation for r_1 into it to obtain that

$$r_2 = b - q_2 r_1 = b - q_2 (a - q_1 b) = (1 + q_2 q_1) b - q_2 a.$$

Thus, r_2 is also a linear combination of a and b. Next, if there is a third equation, use it and our earlier linear combinations to obtain r_3 as a linear combination of a and b:

$$\begin{aligned} r_3 &= r_1 - q_3 r_2 = a - q_1 b - q_3 ((1 + q_2 q_1) b - q_2 a) \\ &= (1 + q_3 q_2) a - (q_1 + q_3 + q_3 q_2 q_1) b. \end{aligned}$$

And so forth: Given r_{k-1} and r_k are linear combinations of a and b, we can use the $(k+1)$th equation to express r_{k+1} as a linear combination of a and b. So continuing in this fashion, the final equation yields r_n as a linear combination of a and b. We know from Theorem 2 that the last remainder, $r_n = \gcd\{a, b\}$, so we are done. □

Example 3. Let $a = 2498$, $b = 314$, $d = \gcd\{a, b\}$. Find d and integers m and n for which $ma + nb = d$.

Solution. To avoid mixing numbers, let's keep the symbolic forms of 24987 and 314. Now apply the Euclidean Algorithm to obtain

$$\begin{aligned} a &= 7 \cdot b + 300 \\ b &= 1 \cdot 300 + 14 \\ 300 &= 21 \cdot 14 + 6 \\ 14 &= 2 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

Rewrite these equations by solving for remainders as in Theorem 3 with simplifications as we go:

$$\begin{aligned} a - 7b &= 300 \\ b - 1 \cdot (a - 7b) = -a + 8b &= 14 \\ a - 7b - 21 \cdot (-a + 8b) = 22a - 175b &= 6 \\ -a + 8b - 2 \cdot (22a - 175b) = -45a + 358b &= 2. \end{aligned}$$

And check our answer: $-45 \cdot 2498 + 258 \cdot 314 = 2$. Check!

□

Here are a few more basic theorems from number theory:

Theorem 4. *Let a, b and c be integers such that a and b are relatively prime and $a \,|bc$. Then $a \,|c$.*

Proof. Since a and b are relatively prime, Theorem 3 tells us that there exist integers m and n such that $ma + nb = 1$. Multiply both sides by c and get $mac + nbc = c$. Now certainly $a \,|a$ and we're given that $a \,|bc$. So $bc = ap$ for some integer p. Plug this into the equation for c and obtain that

$$c = mac + nbc = mac + nap = a\,(mc + np)\,.$$

Hence, $a \,|c$. □

The next two theorems aren't needed in what follows them, but they're very classical theorems for which we've done enough work that their demonstrations are fairly straightforward.

Theorem 5. *(Fundamental Theorem of Arithmetic) Every non-prime natural number greater than* 1 *can be factored into a product of primes that is unique, up to order of terms.*

Proof. Let c be a non-prime natural number greater than 1. Then we must be able to factor $c = ab$ as a product of smaller natural numbers a and b. If a or b is not 1, then apply this process to them to obtain still smaller factors of a and b, hence factors of c. Now repeat this process on all factors until we reach factors that are natural numbers with no divisors other than 1 and themselves. This must occur since there are only a finite number of numbers between 1 and n. Each of these final factors is, by definition, a prime or 1. Thus, we have shown that c is a product of primes.

For uniqueness, let's suppose that uniqueness fails for some natural number. Then there is a smallest natural number $a > 1$ for which uniqueness fails. So write a as a product of primes in two different ways, say

$$p_1p_2p_3 \cdots p_m = a = q_1q_2q_3 \cdots q_n, \tag{1}$$

where the p_i's and q_j's are primes. If there is a prime on the left side that does not occur on the right side, say p_i, then $p_i \,|q_1q_2 \cdots q_n$ but p_i does not divide the different prime q_1, and so $\gcd\{p_i, q_1\} = 1$. By Theorem 4 we must have that $p_i \,|q_2q_3 \cdots q_n$. We can repeat this argument over and over until there is only one prime left. Hence, $p_i \,|q_n$ which is a contradiction since these are distinct primes. It follows that there is some prime that occurs on both sides of Equation (1). In this case we can rearrange the primes on both sides so that the common prime

is the first one listed, that is, $p_1 = q_1$. Do so and cancel p_1 from both sides of the equation to obtain that the natural number $b = a/p_1$ satisfies the equation

$$p_2 p_3 \cdots p_m = \frac{a}{p_1} = b = q_2 q_3 \cdots q_n, \tag{2}$$

However, b is smaller than a, so must be a number with unique factorization. This means that every prime that occurs on one side of the equation occurs on the other exactly the same number of times. In particular, if the prime p_1 re-occurs on the left side of Equation (2), it does so the same number of times on the right. So when we multiply Equation (2) by p_1 we simply obtain Equation (1) again. But every prime on one side occurs the same number of times on the other. Therefore, the two factorizations of a are identical, contrary to our hypothesis. So there is no natural number for which unique factorization into primes fails, which proves the theorem. □

Theorem 6. *There are infinitely many prime numbers.*

Proof. We leave this as an exercise with hints (see Exercise 8). □

Question: Can we find rational approximations to any irrational number that are as good as we like? For example, given that $\pi = 3.1415926525358\ldots$, $22/7 = 3.142857\cdots$ is is an approximation of π good to 3 digits, which is sufficient for some calculations. But $355/113 = 3.141592920\cdots$ is even better, good to 7 digits. Can we do still better, that is, as much as we like? The problem of approximating irrational numbers by rationals is ancient. Here's a generic statement about what has been known for a long time, namely that the rational numbers are dense in the set of real numbers. Think decimal representation and it's pretty obvious, but what follows is a more traditional decimal-free demonstration of a slightly more specific statement:

Theorem 7. *Let $q_1, q_2, q_3, \ldots q_k \ldots$ be any unbounded sequence of natural numbers. Then the set of rational numbers of the form p/q_k, with p an integer not divisible by q_k, is dense in the set of real numbers..*

Proof. Form the infinite grid of points p/q_k, where p is any integer. Now remove the points at which p is divisible by q. This simply excludes integer points from the grid of all points p/q_k for integers $p = 0, \pm 1, \pm 2, \ldots$. Therefore, the distance between any two adjacent points is therefore at most $2/q_k$ rather than $1/q_k$. Now any real number α fits between two adjacent points in our revised grid for a given k , so we must have that for some integer p not a multiple of q that $|\alpha - p/q_k| < 2/q_k$. But we can make $2/q_k$ as small as we want by choosing a sufficiently large index k, since the numbers q_k are unbounded. Since α was any real number, we conclude that these rational numbers are dense in the reals. □

Comments:

(a) Note that since integers are excluded, the only fractions p/q_k in the preceding proof that occur in the interval $[0, 1]$ are those for which $1 \leq p < q_k$. Therefore, if the sequence of q_k's is unbounded, these fractions are dense in the interval $[0, 1]$.

(b) There is an even stronger converse to this theorem: If the set of all the fractions p/q_k approximates a *single* irrational number α arbitrarily well, then the sequence of denominators q_k must be unbounded. To see this, recall that $\alpha = \lfloor \alpha \rfloor + \{\alpha\}$ and $\lfloor \alpha \rfloor$ is an integer, so we can certainly approximate the irrational $\{\alpha\} = \alpha - \lfloor \alpha \rfloor$ (see Exercise 11) arbitrarily well too. So use $\{\alpha\}$ in place of α and we can assume that $0 < \alpha < 1$. Now the only rational numbers that we need are fractions smaller than one. These have the form p/q_k where $1 \leq q < q_k$ and $k = 1, 2, 3, \ldots$. If there were an upper bound on the numbers q_k, say all $q_k < Q$, then there would at most Q distinct denominators, hence only a finite number of fractions p/q_k with $1 \leq p < q_k$. None of these numbers is irrational, so the absolute difference between them and α is positive. That would imply that none of the fractions can never get closer to α than the smallest of these differences. Hence, the only way for the set of these fractions p/q_k to approximate α arbitrarily well is for the denominators q_k to be unbounded.

The Punch Lines

OK, back to our main story line. Let's begin with some irrational numbers that we'll find useful in later discussion.

Theorem 8. *Let p be a prime number. Then $\log p$ is irrational.*

Proof. This one I'll leave to the reader as homework assignment (Exercise 8) – assume otherwise, that is, $\log p = m/n$, eliminate fractions, remind yourself of the definition of common (base 10) logs, unwrap it, and come to a contradiction! □

A clear understanding of the methods and limits of ancient techniques such as the Euclidean algorithm and its cousin continued fractions had to wait until the 18th-19 th centuries. What follows is a more precise statement of what can be said in general. Burger gave a charming "example proof" of the following theorem in course Lecture 21 using the " Pigeonhole Principle" which roughly says that if $n + 1$ objects are tossed into n boxes, then at at least one of the boxes contains two or more objects. Let's abstract his proof for picky readers like myself:

Theorem 9. *(Gustav Dirichlet, 1842) Let α be a real number amd $Q > 1$ a natural number. Then ther exists a rational number p/q such that $|\alpha - p/q| \leq 1/\left((Q+1)\, q\right)$ and $1 \leq q \leq Q$.*

Proof. If p/q is close to a positive real number α, then $-p/q$ is just as close to $-\alpha$; so it suffices to consider only positive reals. Let the positive real number α and natural number $Q > 1$ be given. Divide the interval $[0, 1]$ into $Q + 1$ subintervals of equal length $\frac{1}{Q+1}$ between the points $0 = \frac{0}{Q+1}, \frac{1}{Q+1}, \frac{2}{Q+1}, \frac{3}{Q+1}, \ldots, \frac{Q}{Q+1}, \frac{Q+1}{Q+1} = 1$. Now consider the $Q + 2$ numbers $k\alpha = \lfloor k \cdot \alpha \rfloor + \{k \cdot \alpha\}$, for $k = 0, 1, \ldots, Q + 1$. Notice that the $Q+2$ numbers $\{0 \cdot \alpha\}$, $\{1 \cdot \alpha\}$, $\{2 \cdot \alpha\}$, ..., $\{Q \cdot \alpha\}$, $\{(Q + 1) \cdot \alpha\}$ all live in the interval $[0, 1]$, so each of these $Q + 2$ numbers fits into one of the $Q+1$ subintervals defined above. Hence, by the Pigeonhole Principle, at least two of them must live in the same subinterval and therefore be at most $\frac{1}{Q+1}$ apart, let's say $\{m\alpha\}$ and $\{n\alpha\}$ with $m > n$, so that $|\{m\alpha\} - \{n\alpha\}| \leq 1/(Q + 1)$. Next, set $m - n = q > 0$. Recall that for any positive real number β, we have $\{\beta\} = \beta - \lfloor \beta \rfloor$. In our case we we define the integer p by $p = \lfloor m \cdot \alpha \rfloor - \lfloor n \cdot \alpha \rfloor$ and obtain

$$\begin{aligned} |\{m\alpha\} - \{n\alpha\}| &= |m\alpha - \lfloor m\alpha \rfloor - (n\alpha - \lfloor n\alpha \rfloor)| \\ &= |m\alpha - n\alpha - \lfloor m\alpha \rfloor + \lfloor n\alpha \rfloor| \\ &= |(m - n)\,\alpha - (\lfloor m\alpha \rfloor - \lfloor n\alpha \rfloor)| \\ &= |q\alpha - p| \\ &= q\,|\alpha - p/q| < 1/\,(Q + 1)\,. \end{aligned}$$

If p were negative, we would have $|\alpha - p/q| > |\alpha| = |\alpha - 0/p|$ so that $p = 0$ satisfies the inequality as well, so we can assume that p is nonnegative. Divide both sides by q and the inequality of the theorem follows. □

In Lecture 21, Professor Burger commented without proof that since we know that $\log 2$ is irrational (2 is a prime, see above), we can apply Kronecker's theorem (also stated without proof) to $\alpha = \log 2$ to prove the SSN claim at the beginning of this essay (also stated without proof). Here are my elementary (remember, that doesn't necessarily mean easy, just not requiring fancy mathematics background) proofs of both comments They took a bit more time than I'd anticipated but hey, I'm a mathematician, couldn't resist and enjoyed the challenge of coming up with proofs on my own:

Theorem 10. *(Leopold Kronecker, 1884) Let α be an irrational number. Then the infinite sequence of numbers $\{\alpha\}$, $\{2\alpha\}$, $\{3\alpha\}$, $\{4\alpha\}$, ... is dense in the interval $[0, 1]$.*

Proof. Begin by applying Dirichlet's theorem to α and an arbitrary natural number $Q > 1$ to obtain that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{(Q + 1)}\frac{1}{q}. \tag{1}$$

for integers p and $1 \leq q \leq Q$. We can assume that p and q are relatively prime; for if not, say $d = \gcd\{p, q\}$, so that $p = p'd$, $q = q'd$. It follows that

$$\left|\alpha - \frac{p}{q}\right| = \left|\alpha - \frac{p'd}{q'd}\right| = \left|\alpha - \frac{p'}{q'}\right| \leq \frac{1}{(Q+1)\,q'd} \leq \frac{1}{(Q+1)\,q'}$$

with $q' \leq q \leq Q$. So we may as well take $p = p'$ and $q = q'$ to begin with. Now multiply both sides by m, where $1 \leq m < q$ to obtain that

$$\left|m\alpha - \frac{mp}{q}\right| \leq \frac{1}{(Q+1)}\frac{m}{q}. \tag{2}$$

We claim that there cannot be any integer between $m\alpha$ and mp/q. For if there were such an integer, say n, then n would be closer to mp/q than $m\alpha$ is, and thus

$$\left|n - \frac{mp}{q}\right| \leq \frac{1}{(Q+1)}\frac{m}{q}.$$

Multiply both sides by q to obtain that

$$|nq - mp| \leq \frac{m}{(Q+1)} < \frac{m}{q} < 1.$$

However, both nq and mp are integers whose difference is smaller than 1. Thus, they must be equal, that is, $nq = mp$. This means that $q \,|mp$. However, q and p are relatively prime, and so by Theorem 4, $q \,|m$. But $m < q$, so this is impossible. Therefore, there is no integer n between $m\alpha$ and mp/q.

Now recall that for any real number β, we have $\lfloor\beta\rfloor + \{\beta\}$. Use this expression for both terms on the left-hand side of Equation (2) to obtain

$$\left|\lfloor m\alpha\rfloor + \{m\alpha\} - \left(\left\lfloor\frac{mp}{q}\right\rfloor + \left\{\frac{mp}{q}\right\}\right)\right| \leq \frac{1}{(Q+1)}\frac{m}{q}.$$

We have shown that there are no integers between $m\alpha$ and mp/q. Therefore, they have the same floors, that is, $\lfloor m\alpha\rfloor = \lfloor mp/q\rfloor$. So these two term cancel, and what remains is

$$\left|\{m\alpha\} - \left\{\frac{mp}{q}\right\}\right| \leq \frac{1}{(Q+1)}\frac{m}{q}$$

for $1 \leq m < q$.

Let's take a closer look at the fractions $\{mp/q\}$. For each integer m we can use the Division Algorithm $mp = s_m q + r_m$, where quotient s_m and remainder r_m vary with m. We know that $0 \leq r_m < q$. However, r_m cannot be 0, for that would that $mp = s_m q$, which in turn would imply $q \,|mp$ which, as we have already seen, is impossible. Therefore, none of the remainders r_m are 0. On the other hand, none of the remainders are equal to each other, for if so, say $r_m = r_n$ with $m > n$,

subtract the two instances of the Division Algorithm that define the remainders and obtain

$$\begin{aligned} mp - np &= s_m q + r_m - s_n q - r_n \\ (m-n)\, p &= s_m q - s_n q = (s_m - s_n)\, q. \end{aligned}$$

which implies that $q \,|(m-n)$ by Theorem 4 again. Since $m-n$ is a positive number smaller than q, this is impossible. Thus, all the remainders are distinct, as claimed. Since there are exactly $q-1$ remainders, all between 1 and $q-1$, the remainders consists of all the numbers between 1 and $q-1$ in some rearranged order. It follows that we can match up fractional parts $\{\alpha\}$, $\{2\alpha\}$, $\{3\alpha\}$, ... $\{(q-1)\,\alpha\}$ with rational numbers $1/q$, $2/q$, $3/q$, ... , $(q-1)\,/q$ in some rearranged order such that if $m\alpha$ is matched with k/q, then since $0 < m < q < Q+1$

$$\left| \{m\alpha\} - \frac{k}{q} \right| \leq \frac{1}{(Q+1)} \frac{m}{q} < \frac{1}{q}.$$

Next, let β be any real number in the interval $[0,1]$. Then β must be between two adjacent fractions $0 < 1/q < 2/q < \cdots < (q-1)/q < 1$ and therefore for some integer k between 1 and $q-1$ we have that $|\beta - k/q| \leq 1/q$. If that fraction is matched up with $\{m\alpha\}$ as above, then

$$|\{m\alpha\} - \beta| = \left| \{m\alpha\} - \frac{k}{q} + \frac{k}{q} - \beta \right| \leq \left| \{m\alpha\} - \frac{k}{q} \right| + \left| \frac{k}{q} - \beta \right| \leq \frac{1}{q} + \frac{1}{q} = \frac{2}{q}. \quad (3)$$

Finally, suppose we apply the preceding analysis not just to one positive Q, but to an unbounded sequence $Q_1, Q_2, Q_3, \ldots Q_k, \ldots$ of natural numbers. According to Equation (1), we can obtain approximations p_k/q_k to α within $1/Q_k$. This means that α can be approximated arbitrarily well by such fractions. Comment (b) following Theorem 7 tells us that the sequence of denominators $q_1, q_2, q_3, \ldots$ that we choose must therefore be unbounded. Equation (3) shows that, for a suitable choice of m depending on q_k, we have $|\{m\alpha\} - \beta| \leq 2/q_k$. But the q_k's are unbounded, so we can find fractional parts $\{m\alpha\}$ arbitrarily close to β. Thus, any real number β with $0 \leq \beta \leq 1$ can be approximated arbitrarily well by numbers from the sequence of numbers $\{\alpha\}$, $\{2\alpha\}$, $\{3\alpha\}$, $\{4\alpha\}$, ... Therefore, this sequence is dense in the interval $[0,1]$. □

And now we've come full circle back to the powers of 2. Actually, more is true and it's about as much work to prove this for any prime p as it is for 2:

Theorem 11. *For any natural number M and prime number p there exists a natural number N such that the digits of M are exactly the leading digits of p^N.*

Proof. For starters, if the number M is a pure power of p, we are done. Otherwise, we may extend M a bit: If the old M has decimal form $M = a_1 a_2 \cdots a_k$, with

$a_k = 0$ or 9, then our new and improved M will have the decimal form $M = a_1 a_2 \cdots a_k 1$. If the leading digits of p^N match these digits, then they certainly match the digits of the old M. So this modification is harmless and it has another virtue, namely that it ensures that $\lfloor \log M \rfloor = \lfloor \log (M+1) \rfloor$. For neither log is an integer, since this would mean that M or $M+1$ would have decimal form ending in the digit 0, which they do not. Moreover, there is no integer n between these logs, for then we would have $\log M < n < \log (M+1)$. This would imply that $10^{\log M} < 10^n < 10^{log(M+1)}$, that is, $M < 10^n < M+1$. Since M and $M+1$ are successive integers, this is impossible. Thus, $\lfloor \log M \rfloor = \lfloor \log (M+1) \rfloor$.

Next, use the fact that

$$\log M = \lfloor \log M \rfloor + \{\log M\} < \lfloor \log (M+1) \rfloor + \{\log (M+1)\} = \log (M+1)$$

and subtract the equal integer part from both sides of the middle inequality to obtain that $\{\log M\} < \{\log (M+1)\}$. Both of these fractional parts are in the interval $[0,1]$. Now for the key part: the midpoint of these two numbers can be approximated arbitrarily well by a number of the form $\{n \log p\}$ with n a natural number, since $\log p$ is irrational (Theorem 8) and numbers of that form are dense in the interval $[0,1]$ (Theorem 10). Therefore, we can find a natural number N such that $\{N \log p\}$ is strictly between $\{\log M\}$ and $\{\log (M+1)\}$, that is, $\{\log M\} < \{N \log p\} < \{\log (M+1)\}$. Put another way we have

$$\log M - \lfloor \log M \rfloor < N \log p - \lfloor N \log p \rfloor < \log (M+1) - \lfloor \log (M+1) \rfloor .$$

Now add $\lfloor \log M \rfloor$, which is equal to $\lfloor \log (M+1) \rfloor$, to all three terms of the inequality to obtain

$$\log M < N \log p - \lfloor N \log p \rfloor + \lfloor \log M \rfloor < \log (M+1) .$$

Next, set $m = \lfloor N \log p \rfloor - \lfloor \log M \rfloor$ so that the middle term becomes $N \log p - m$. Raise 10 to the powers of each of the terms in this last form of the inequalities to obtain the inequalities

$$M = 10^{\log M} < 10^{N \log p - m} = \left(10^{\log p}\right)^N \cdot 10^{-m} = p^N \cdot 10^{-m} < 10^{\log (M+1)} = M+1.$$

Now take the integer parts of each term, noting that M and $M+1$ are adjacent integers and the middle term is strictly in-between, so we must have

$$M = \left\lfloor p^N \cdot 10^{-m} \right\rfloor .$$

From this we see that we must have $m \geq 0$. For otherwise $p^N \cdot 10^{-m}$ would already be an integer equal to M and whose decimal form end in the digit 0, which is not true of M. This is exactly what we want since taking the integer part of $p^N \cdot 10^{-m}$ now amounts to chopping off the last m digits of p^N and what remains is M. $\square$

Postscripts

I thoroughly enjoyed the Great Course "Introduction to Number Theory" by Professor Burger. Let me qualify that: Professor Burger assumes that his listeners have long forgotten their high school algebra, which is exactly the right thing to do here, since you are speaking to non-specialists who may have had nothing to do with mathematics for many years. I realized that and fully expected some explanations of materials to be extremely boring (to me). I was not disappointed in that respect (hey, I am a retired mathematician!), but I can assure the non-specialists that you will enjoy this delightful elementary introduction to a beautiful area of mathematics. My own motivation was primarily to refresh my memory of some terminology and concepts of number theory and perhaps learn a bit more of the historical background that we professionals (well, me anyway) tend to ignore. Again, I was not disappointed. Thank you Professor Burger for an enjoyable time and for inspiring this essay by way of the "powers of 2" fun fact that you introduced in Lecture 2 of your course.

I was a bit surprised towards the end of "Introduction to Number Theory" when I was introduced to some theorems in number theory that I either did not know or had long forgotten. For one, though I vaguely remembered Euler's Product Formula in Lecture 8 (think I used it in an undergraduate honors seminar some forty five years ago when I was introducing the topic of infinite products), I was pleasantly surprised to see how a slight variation turned it into the Riemann zeta funtion. Let me add that Professor Burger's exposition was elegantly clear.

For another, I found the lectures on Diophantine approximation in and continued fracctions in Lectures 21-23 to be quite fascinating. (So much so that I amused myself by writing routines in my favorite calculator, ALAMA Calculator, that construct and deconstruct continued fraction approximations to a real number – not entirely routine thanks to the vicissitudes of wanting pure integer arithmetic but restricted to using finite precision floating point arithmetic.)

Remark. About how I uncovered the proof to Kronecker's Theorem: This one had me stumped for a bit, so I turned to ALAMA calculator and did some numerical experiments to locate rational fractions satisfying Dirichlet's Theorem as applied to a few irrational numbers such as $\{\pi\}$, $\log 2$ and $\{\log 99.5\}$. I then examined differences between floors of multiples of these numbers and floors of their differences. Some patterns made it clear to me how a proof of the theorem could proceed. Interestingly enough, most of the rational fractions that I found were values of continued fractions such as Professor Burger covered in Lectures 21-23.

My point is not that I found a proof, it's how I did it. Worthwhile mathematical problems are not usually easy. And solutions usually don't spring from a

mathematician's head like Athena from Zeus's. Rather, it takes experimentation with special cases, trial and error, study and even a bit of luck. It's good old fashioned work that can be deeply satisfying. As K. F. Gauss put it: "It is not knowledge, but the act of learning, not possession but the act of getting there, which grants the greatest enjoyment."

Exercises

Exercise 1. Apply the division algorithm to the following dividend a and quotient b:

(a) $a = 4322$, $b = 282$ (b) $a = 48$, $b = 196$ (c) $a = 3640$, $b = 234$.

Exercise 2. Complete the proof of Theorem 1 by dealing with the case that both a and b are negative.

Exercise 3. Find the greatest common divisor d of a and b as in Exercise 1 and use your work to find integers m and n such that $ma + nb = d$.

Exercise 4. Show that Theorem 3 holds in the case that $r_1 = 0$.

Exercise 5. Prove the 2/3 rule: If a, b and c are integers such that $a = b + c$ and the integer d divides two of the three integers, then it divides the third one.

Exercise 6. One way to completely factor a natural number n is to list the primes less than n in order and for each such prime, divide n by it and continue this process until the current prime does not divide the remaining number, then move on to the next prime. Use this method to determine the prime factorization of $n = 6120$. (Do not do a complete list of primes first. Build the list as you go.)

Exercise 7. If one uses the method of Exercise 6 to factor a number n, we need only consider primes p for which $p \leq \sqrt{n}$. Show why this is true.

Exercise 8. Prove Theorem 6 by assuming that it is false and enumerating all of the primes, say as p_1, p_2, p_3, ... p_n. Then consider the number $n = p_1 p_2 p_3 \cdots p_n + 1$ and apply the Fundamental Theorem of Arithmetic to it.

Exercise 9. Show that if real numbers a and b satisfy $a < b$, then $\lfloor a \rfloor \leq \lfloor b \rfloor$.

Exercise 10. Prove Theorem 8.

Exercise 11. Show that if α is irrational, then so is $\{\alpha\}$.

Exercise 12. Take $p = 2$. The proof of Theorem 11 actually shows you what exponent N to search for, but there can be an extremely tight fit for the right fractional part $\{N \log 2\}$. Determine the width of the interval into which this fractional part must fit in the worst case SSN. (First, make sure you know what that is.)

Exercise 13. Use the proof of Theorem 11 to find the correct power of 2 whose leading digits are those of M, where

(a) $M = 11$ (b) $M = 123$ (c) $M = 1123$