Number Theory

Everything else

Misha Lavrov

ARML Practice 10/06/2013
PUMaC, 2009. How many positive integer pairs \((a, b)\) satisfy 
\[a^2 + b^2 = ab(a + b)\]?
PUMaC, 2009. How many positive integer pairs \((a, b)\) satisfy \(a^2 + b^2 = ab(a + b)\)?

Let \(p\) be a prime. Let \(p^x\) be the highest power of \(p\) dividing \(a\), and \(p^y\) be the highest power of \(p\) dividing \(b\).
Solving integer equations using divisors

PUMaC, 2009. How many positive integer pairs \((a, b)\) satisfy \(a^2 + b^2 = ab(a + b)\)?

1. Let \(p\) be a prime. Let \(p^x\) be the highest power of \(p\) dividing \(a\), and \(p^y\) be the highest power of \(p\) dividing \(b\).

2. Suppose \(x < y\). Then \(p^{2x}\) is the highest power dividing \(a^2 + b^2\), \(p^{x+y}\) is the highest power dividing \(ab\), and \(p^x\) is the highest power dividing \(a + b\).
PUMaC, 2009. How many positive integer pairs \((a, b)\) satisfy \(a^2 + b^2 = ab(a + b)\)?

1. Let \(p\) be a prime. Let \(p^x\) be the highest power of \(p\) dividing \(a\), and \(p^y\) be the highest power of \(p\) dividing \(b\).

2. Suppose \(x < y\). Then \(p^{2x}\) is the highest power dividing \(a^2 + b^2\), \(p^{x+y}\) is the highest power dividing \(ab\), and \(p^x\) is the highest power dividing \(a + b\).

3. So \(p^{2x} = p^{2x+y}\), which means \(y = 0\). But \(x < y\), so this is impossible. So we can’t have \(x < y\); we can’t have \(x > y\) for the same reason, so \(x = y\).
PUMaC, 2009. How many positive integer pairs \((a, b)\) satisfy \(a^2 + b^2 = ab(a + b)\)?

1. Let \(p\) be a prime. Let \(p^x\) be the highest power of \(p\) dividing \(a\), and \(p^y\) be the highest power of \(p\) dividing \(b\).

2. Suppose \(x < y\). Then \(p^{2x}\) is the highest power dividing \(a^2 + b^2\), \(p^{x+y}\) is the highest power dividing \(ab\), and \(p^x\) is the highest power dividing \(a + b\).

3. So \(p^{2x} = p^{2x+y}\), which means \(y = 0\). But \(x < y\), so this is impossible. So we can’t have \(x < y\); we can’t have \(x > y\) for the same reason, so \(x = y\).

4. This is true for all \(p\), so \(a = b\). Then \(2a^2 = a^2(a + a) = 2a^3\), so \(a = b = 1\).
AIME, 1991. How many fractions $\frac{a}{b}$ are there, for which $ab = 20!$ (when written in simplest terms)? How many of these satisfy $0 < \frac{a}{b} < 1$?

Ukrainian MO, 2002. Solve

$$n^{2002} = m(m + n)(m + 2n) \cdots (m + 2001n)$$

for integers $m, n$.

British MO, 2002. Find all solutions in positive integers $a, b, c$ to the equation $a! \cdot b! = a! + b! + c!$.

Putnam, 2000. Prove that the expression $\frac{\gcd(n,k)}{n} \binom{n}{k}$ is an integer for all pairs of integers $n \leq k \leq 1$. 
AIME, 1991. We can factor

\[ 20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19. \]

(What’s important here is that there are 8 primes that appear in the factorization of \( 20! \), which are the 8 primes \( \leq 20 \).)

If \( ab = 20! \) and \( \frac{a}{b} \) is in simplest terms (that is, \( \gcd(a, b) = 1 \)) then each prime number must go entirely in \( a \) or entirely in \( b \). There are 2 possibilities for each prime, and eight primes, so that’s \( 2^8 = 256 \) choices.

How many are between 0 and 1?
AIME, 1991. We can factor

\[ 20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19. \]

(What’s important here is that there are 8 primes that appear in the factorization of 20!, which are the 8 primes \( \leq 20 \).)

If \( ab = 20! \) and \( \frac{a}{b} \) is in simplest terms (that is, \( \gcd(a, b) = 1 \)) then each prime number must go entirely in \( a \) or entirely in \( b \). There are 2 possibilities for each prime, and eight primes, so that’s \( 2^8 = 256 \) choices.

How many are between 0 and 1?

We always have \( \frac{a}{b} > 0 \), and either \( \frac{a}{b} < 1 \) or \( \frac{b}{a} < 1 \). Therefore the answer is 128: half of the total number of fractions.
Ukrainian MO, 2002. Let $p$ be a prime. Then:

- If $p$ divides $m$, then $p$ divides the RHS, so $p$ divides the LHS, which is $n^{2002}$. Therefore $p$ divides $n$.

- If $p$ divides $n$, then $p$ divides the LHS, so $p$ divides the RHS, which means $p$ divides $m + kn$ for some $k$. Since $p$ also divides $kn$, $p$ must divide $m$. 
Ukrainian MO, 2002. Let $p$ be a prime. Then:

- If $p$ divides $m$, then $p$ divides the RHS, so $p$ divides the LHS, which is $n^{2002}$. Therefore $p$ divides $n$.

- If $p$ divides $n$, then $p$ divides the LHS, so $p$ divides the RHS, which means $p$ divides $m + kn$ for some $k$. Since $p$ also divides $kn$, $p$ must divide $m$.

Normally, we’d refine this approach to show that the same power of $p$ divides $m$ and $n$. Here, there is a shortcut: If $m$ and $n$ are solutions, so are $\frac{m}{p}$ and $\frac{n}{p}$. Unless $m = n = 0$, we can keep dividing by $p$ until one is no longer divisible by $p$; but then the other can’t be divisible by $p$ either.

In any case, we prove $m = n$; but the only solution of this kind is $m = n = 0$. 
British MO, 2002. Ruling out $0 \leq a \leq 2$ and $0 \leq b \leq 2$, $a! \cdot b!$ is much larger than $a!$ or $b!$, so $c$ is the largest of the three integers.

Next, we show that $a! = b!$. Suppose $a! < b!$: then $b!$ is divisible by $(a + 1)!$, and if we write

$$a! \cdot b! - b! - c! = a!$$

then everything on the left is divisible by $(a + 1)!$, while $a!$ is not. This is impossible.

Now we have $a!^2 = a! + a! + c!$, or $a!(a! - 2) = c!$. Since $a! - 2$ is not divisible by 3, $a!$ and $c!$ must have the same number of factors of 3, so $c = a + 1$ or $c = a + 2$. Checking both, we get a single solution:

$$3! \cdot 3! = 3! + 3! + 4!$$
Putnam, 2000. Our goal is to show that $\gcd(n, k) \binom{n}{k}$ is divisible by $n$.

For all primes $p$, suppose $p^x$ divides $n$ and $p^y$ divides $k$. If $x \leq y$ then all is good, because at $\gcd(n, k) \binom{n}{k}$ is divisible by $p^x$.

If $x > y$, we can use the following trick: $\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}$, and so we can rewrite

$$\frac{\gcd(n, k)}{n} \binom{n}{k} = \frac{\gcd(n, k)}{k} \binom{n-1}{k-1}.$$

Now we have only a power $p^y$ in the denominator, and at least $p^x$ in the numerator, so no power of $p$ is left in the denominator, and we are done.
The totient function

The “totient”, or Euler’s \( \phi \), is defined to be:

\[
\phi(n) = \text{The number of } k, 1 \leq k \leq n, \text{ so that } \gcd(n, k) = 1.
\]

Exercise. Find \( \phi(10000) \).

PUMaC, 2010. Find the largest positive integer \( n \) such that \( n\phi(n) \) is a perfect square.
The totient function

The “totient”, or Euler’s \( \phi \), is defined to be:

\[
\phi(n) = \text{The number of } k, \ 1 \leq k \leq n, \ \text{so that } \gcd(n, k) = 1.
\]

**Exercise.** Find \( \phi(10000) \).

- Easy answer: \( \gcd(10000, k) = 1 \) if \( k \) ends in 1, 3, 7, or 9. There are 4000 such numbers between 1 and 10000.

- General answer: Out of 10000 integers, \( \frac{1}{2} \) are divisible by 2, and \( \frac{1}{5} \) are divisible by 5, so there are \( 10000 \left( 1 - \frac{1}{2} \right) \left( 1 - \frac{1}{5} \right) = 4000 \) left.

**PUMaC, 2010.** Find the largest positive integer \( n \) such that \( n\phi(n) \) is a perfect square.

Using the “general answer” above, it’s easy to see \( n\phi(n) \) can’t be a perfect square for \( n > 1 \).
Rule for raising something to a power mod $m$

**Theorem (Euler’s theorem)**

For all positive integers $a$, $n$ with $\gcd(a, n) = 1$,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

and therefore

$$a^m \equiv a^m \pmod{\phi(n)} \pmod{n}.$$

Intuition: If $\gcd(a, 10) = 1$, then there are $\phi(10) = 4$ digits $a$ can end in: 1, 3, 7, and 9. The powers of $a$ will cycle through these digits: for example, when $a = 3$, we have

$$3^0 = 1, \quad 3^1 = 3, \quad 3^2 = 9, \quad 3^3 = 27 \equiv 7, \quad 3^4 = 81 \equiv 1, \ldots$$
Theorem (Euler’s theorem)

For all positive integers $a$, $n$ with $\gcd(a, n) = 1$,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

and therefore

$$a^m \equiv a^{m \mod \phi(n)} \pmod{n}.$$ 

Intuition: If $\gcd(a, 10) = 1$, then there are $\phi(10) = 4$ digits $a$ can end in: 1, 3, 7, and 9. The powers of $a$ will cycle through these digits: for example, when $a = 3$, we have

$$3^0 = 1, \quad 3^1 = 3, \quad 3^2 = 9, \quad 3^3 = 27 \equiv 7, \quad 3^4 = 81 \equiv 1, \ldots$$

If $\gcd(a, n) \neq 1$, then powers of $a$ eventually repeat every $\phi(n)$ steps, but this is trickier to use.
Competition problems

(Note: this theorem is also useful for small things, like knowing that \(1^4 \equiv 2^4 \equiv 3^4 \equiv 4^4 \equiv 1 \pmod{5}\) last week. These are problems where Euler’s theorem is the main focus.)

Exercise. Compute \(100^{100} \mod 13\).

Texas A&M, 2008. Find the last three digits of \(2007^{2008}\).

VTRMC, 2012. Find the last two digits of \(3^{3^{\ldots^3}}\).

HMMT, 2011. Determine the remainder when

\[
2^{\frac{1 \cdot 2}{2}} + 2^{\frac{2 \cdot 3}{2}} + \cdots + 2^{\frac{2011 \cdot 2012}{2}}
\]

is divided by 7.
Exercise. $100^{100} \equiv (-4)^{100} \equiv (-4)^4 \equiv 9 \pmod{13}$.

Texas A&M, 2008. $2007^{2008} \equiv 7^{2008} \equiv 7^8 \pmod{1000}$. A shortcut for this: $7^2 = 49 = 50 - 1$, so

$$7^8 = (50 - 1)^4 = 50^4 - 4 \cdot 50^3 + 6 \cdot 50^2 - 4 \cdot 50 + 1.$$  

But here, the first three terms are all divisible by 1000, so all we need to worry about is $-4 \cdot 50 + 1 \equiv 801 \pmod{1000}$. 

VTRMC, 2012. Write $3 \uparrow\uparrow n$ for $3^3 \cdot \cdot \cdot^3$ with $n$ 3’s. We use Euler’s theorem recursively: for 100 we need $\phi(100) = 40$, for which we need $\phi(40) = 16$, for which we need $\phi(16) = 8$, for which we need $\phi(8) = 4$, for which we need $\phi(4) = 2$.

Since 3 is odd, $3 \uparrow\uparrow 2007 \equiv 1 \pmod{2}$.

So $3 \uparrow\uparrow 2008 \equiv 3^1 \equiv 3 \pmod{4}$.

So $3 \uparrow\uparrow 2009 \equiv 3^3 \equiv 27 \equiv 3 \pmod{8}$.

So $3 \uparrow\uparrow 2010 \equiv 3^3 \equiv 27 \equiv 11 \pmod{16}$.

So $3 \uparrow\uparrow 2011 \equiv 3^{11} \equiv 27 \pmod{40}$.

So $3 \uparrow\uparrow 2012 \equiv 3^{27} \equiv 87 \pmod{100}$. 
HMMT, 2011. We know $2^n \mod 7$ is determined by $n \mod 6$. But actually, more is true: $2^3 \equiv 1 \pmod{7}$, so $n \mod 3$ is enough.

When looking at $\frac{n(n+1)}{2} \mod 3$, we know either $n - 1$, $n$, or $n + 1$ is divisible by 3. Unless it’s the first, $\frac{n(n+1)}{2}$ is also divisible by 3, in which case $2^{\frac{n(n+1)}{2}} \equiv 1 \pmod{7}$. However, when $n - 1$ is divisible by 3, $\frac{n(n+1)}{2} \equiv 1 \pmod{3}$, and $2^{\frac{n(n+1)}{2}} \equiv 2 \pmod{7}$.

Therefore $2^{\frac{1 \cdot 2}{2}} + 2^{\frac{2 \cdot 3}{2}} + \cdots + 2^{\frac{2011 \cdot 2012}{2}} \mod 7$ simplifies to

$$2 + 1 + 1 + 2 + 1 + 1 + \cdots + 2 \mod 7$$

which is $\frac{2010}{3}(2 + 1 + 1) + 2 \equiv 1 \pmod{7}$. 