UCD MATHEMATICAL ENRICHMENT PROGRAMME 2015.

FEBRUARY 7 2015.

Lecture on PRIME NUMBERS and Functions on INTEGERS.

T. J. LAFFEY.

Recall that if a, b are *integers* and $b > 0$, we can write $a = bq + r$, where q, r are *integers* and $0 \leq r < b$. Then r is called the *remainder* of a on division by b and q the *quotient* of a on division by b.

We say that b divides a if $r = 0$.

So b *divides* a if $a = bq$ for some *integer* q.

The standard algorithm which, given a and b, produces q and r is called *long division*.

Given integers a, b, *not both* zero, there is a greatest integer $d \geqslant 1$ such that d divides a and d divides b.

Every nonzero integer c which divides a and b divides d.

d is called the greatest *common divisor* (gcd) of a and b and also the *highest common factor* (hcf) of a and b.

Examples: $\gcd(48, 27) = 3$, $\gcd(132, 1331) = 11$.

One way to find the gcd of two positive integers is to factorize them as product of primes and then the gcd becomes obvious.

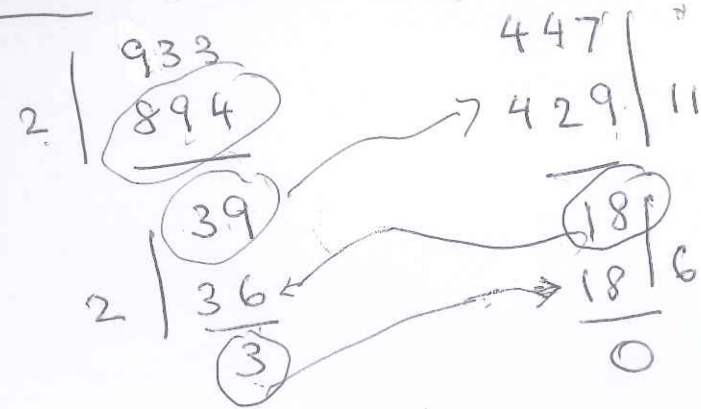
For example, if $a = 2^3 \cdot 3^2 \cdot 7 \cdot 19^2$ and $b = 2^4 \cdot 3 \cdot 19 \cdot 29 \cdot 37$, then

$$\gcd(a, b) = 2^3 \cdot 3 \cdot 19.$$

For large integers, factorization into a product of primes can be a slow process (even with the best known methods and powerful computers with which to implement them). This is one of the key facts underlying security of communication via phone, internet etc.

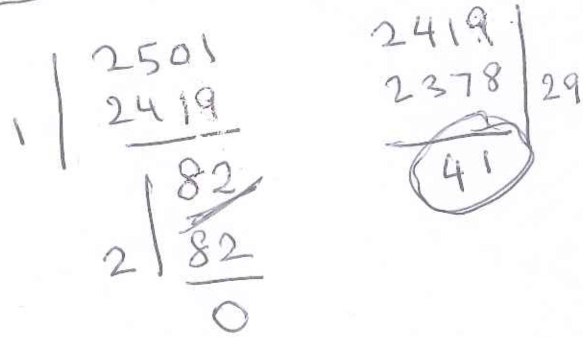
Around 2500 years ago, Euclid discovered a clever way to compute $\gcd(a, b)$ of two given positive integers a, b, which is very efficient and particularly well-designed for implementation on computers. It is called Euclid's algorithm. It is often used to benchmark the speed of computers nowadays.

Example 1. gcd (447, 933).



So gcd (447, 823) = 3.

Example 2 gcd (2501, 2419)



So gcd(2501, 2419) = 41.

We can reverse the process starting with the gcd. In the last example $a = 2501$, $b = 2419$, $d = 41$.

$$d = 41 = \underline{2419} - 29 \times \underline{82} = \underline{2419} - 29 \times (\underline{2501} - \underline{2419})$$
$$= 30 \times \underline{2419} - 29 \times \underline{2501}.$$

In the first example, $a = 933$, $b = 447$, $d = 3$.

$$d = 3 = \underline{39} - 2 \times \underline{18} = \underline{39} - 2 \times (\underline{447} - 11 \times \underline{39})$$
$$= 23 \times \underline{39} - 2 \times \underline{447} = 23 \times (\underline{933} - 2 \times \underline{447}) - 2 \times \underline{447}$$
$$= 23 \times \underline{933} - 48 \times \underline{447}.$$

The procedure generalizes and one gets the following result.

Bézout's Extension of Euclid's Algorithm.

Let a, b be integers not both zero, and let $d = \gcd(a, b)$. Then $d = ax + by$ for some integers x, y.

We return to the infinitude of primes. Last lecture, we discussed Euclid's proof. Another way to proceed is as follows.

Define a sequence as follows $x_1 = 2^{2} - 1$, $x_2 = 2^4 - 1$ and in general $x_k = 2^{2^k} - 1$, $k = 1, 2, 3 \cdots$

Note that
$$x_{k+1} = 2^{2^{k+1}} - 1 = (2^{2^k} - 1)(2^{2^k} + 1)$$
$$= x_k (2^{2^k} + 1),$$

so x_k divides x_{k+1}, for all k.

Let q be a prime dividing $2^{2^k} + 1$. If q divides $x_k = 2^{2^k} - 1$, then q divides $2^{2^k} + 1 - (2^{2^k} - 1) = 2$. But q is odd, so this cannot happen. So for each k, we can find a prime, q_k say, that divides x_{k+1} and doesn't divide x_k, and thus does not divide any x_j $(j \leq k)$. So the sequence $q_1, q_2, \cdots, q_k, \cdots$ yields an infinite sequence of distinct primes.

A totally different proof of the infinitude of primes was obtained by Euler. His idea is as follows: The geometric progression

$$1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots = \frac{1}{1-\frac{1}{p}},$$

for $|p|>1$.

Suppose we consider $\frac{1}{60}=\frac{1}{2^2\cdot 3\cdot 5}$.

Notice that $\frac{1}{60}$ occurs when we multiply

$$\left(1+\frac{1}{2}+\boxed{\frac{1}{2^2}}+\frac{1}{2^3}+\cdots\right)\times\left(1+\boxed{\frac{1}{3}}+\frac{1}{3^2}+\cdots\right)\times\left(1+\boxed{\frac{1}{5}}+\frac{1}{5^2}+\cdots\right).$$

More generally, if a positive integer $n = q_1^{a_1} q_2^{a_2}\cdots q_r^{a_r}$ where $q_1, q_2, \cdots, q_r$ are distinct primes and $a_1, a_2, \cdots, a_n$ are nonnegative integers, then $\frac{1}{n}$ occurs when

$$\left(1+\frac{1}{q_1}+\frac{1}{q_1^2}+\cdots\right), \left(1+\frac{1}{q_2}+\frac{1}{q_2^2}+\cdots\right), \cdots, \left(1+\frac{1}{q_r}+\frac{1}{q_r^2}+\cdots\right)$$

are multiplied.

It follows that if there only finitely many primes, $p_1, p_2, \cdots, p_m$, say every positive integer n would occur in the product

$$\left(1+\frac{1}{p_1}+\frac{1}{p_1^2}+\cdots\right)\left(1+\frac{1}{p_2}+\frac{1}{p_2^2}+\cdots\right)$$

$$\cdots\left(1+\frac{1}{p_m}+\frac{1}{p_m^2}+\cdots\right),$$

so the sum $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots \leq$

$$\left(\frac{1}{1-\frac{1}{p_1}}\right)\left(\frac{1}{1-\frac{1}{p_2}}\right)\cdots\left(\frac{1}{1-\frac{1}{p_m}}\right)<\infty.$$

But it is known that

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots$$

diverges, that is, it not finite.

[One can see this by noting that by grouping terms

$$1+\frac{1}{2}+\underbrace{\frac{1}{3}+\frac{1}{4}}+\underbrace{\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}}+\underbrace{\frac{1}{9}+\frac{1}{10}+\frac{1}{11}+\frac{1}{12}+\frac{1}{13}+\frac{1}{14}}+\frac{1}{16}$$

$$+\cdots$$

$$+\left(\underbrace{\frac{1}{2^{\ell}+1}+\frac{1}{2^{\ell}+2}}+\cdots+\frac{1}{2^{2\ell}}\right)+\cdots$$

$$>1+\frac{1}{2}+\left(\frac{1}{4}+\frac{1}{4}\right)+\left(\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}\right)+\left(\underbrace{\frac{1}{16}+\frac{1}{16}+\cdots+\frac{1}{16}}_{8\text{ times}}\right)$$

$$+\cdots\left(\underbrace{\frac{1}{2^{2\ell}}+\frac{1}{2^{2\ell}}+\cdots+\frac{1}{2^{2\ell}}}_{2^{\ell}\text{ times}}\right)+$$

$$=1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}$$

$$+\cdots+\frac{1}{2}+$$, the sum

can be made greater than any given number by taking sufficient many terms of the series $1+\frac{1}{2}+\frac{1}{3}+\cdots$]

Euler's proof introduced a new era in the study of the distribution of primes. His introduction of infinite series and convergence into the study of prime numbers led quickly to the use of techniques of calculus, geometry and probability. Famous French mathematicians Lagrange and Laplace and most of all Cauchy, through the development of complex analysis, contributed, as did the German mathematicians, especially Gauss and Riemann, and the Russian mathematician Chebyshev.

The big question they worked on in this area was: what fraction of the numbers $1, 2, \ldots, n$ are primes? They wished to know what this ratio is like as n gets bigger and bigger.

The following major result was proved:

For a positive integer x, let $\pi(x)$ be the number of primes $\leq x$. Then

$$\frac{\pi(x)}{x/\ln(x)} \longrightarrow 1 \quad \text{as} \quad x \longrightarrow \infty.$$

Lagrange and Gauss conjectured the result and, 80 years later, it was proved independently by Hadamard and de la Vallée Poussin.

Suppose $n = q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r}$ is a positive integer, where $q_1, \cdots, q_r$ are distinct primes and $a_1, a_2, \cdots, a_r$ nonnegative integer.

By unique factorization, if m is a positive integer that divides n, then

$$m = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$$

where the integers b_i satisfy $0 \leq b_i \leq a_i$.

Conversely, every such m divides n.

We have a_i+1 choices for b_i (since b_i is one of the a_i+1 numbers $0, 1, 2, \cdots, a_i$), and by unique factorization, different choices of the b_i lead to different factors m.

Hence, the ~~total~~ number of positive integers which divide n is

$$\sigma(n) = (a_1+1)(a_2+1)\cdots(a_r+1).$$

For example 1 billion $= 10^9 = 2^9 \times 5^9$, so the total number of positive integers which divide 1 billion $= (9+1)(9+1) = 100$.

Related to this, we can consider the sum of all the positive integers which divide n. Every such positive integer is of the form

$$m = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$$

If we fix all b_is except b_j, we can vary b_j from 0 to a_j and the sum of the resulting numbers is

$$\sum_{l=0}^{a_j} q_1^{b_1}\cdots q_1^{b_{j-1}}\, q_j^{l}\, q_{j+1}^{b_{j+1}}\cdots q_r^{b_r}$$

$$= q_1^{b_1}\cdots q_1^{b_{j-1}}\left(\sum_{l=0}^{a_j} q_j^{l}\right) q_{j+1}^{b_{j+1}}\cdots q_r^{b_r}$$

$$= q_1^{b_1}\cdots q_1^{b_{j-1}}\left(\frac{q_j^{a_j+1}-1}{q_j-1}\right) q_{j+1}^{b_{j+1}}\cdots q_r^{b_r}.$$

We can then keep all this contribution fixed except for another b_i and continue.

Continuing in this way, we get the result:

The sum $d(n)$ of the (positive) divisors of

$$n = q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r}$$

where $q_1, \ldots, q_r$ are distinct primes and $a_1, \ldots, a_r$ nonnegative integers is the product

$$\prod_{i=1}^{r} \frac{q_i^{a_i+1} - 1}{q_i - 1}.$$

For example, the sum of the divisors of 1 billion is

$$\left(\frac{2^{9+1}-1}{2-1}\right)\left(\frac{5^{9+1}-1}{5-1}\right) = \frac{(2^{10}-1)(5^{10}-1)}{4}.$$

A <u>perfect number</u> is an integer $n > 1$ with $d(n) = 2n$. The sequence of perfect numbers begin 6, 28, 496, ...

6 has (positive) divisors 1, 2, 3, 6 and $1+2+3+6=12$,

28 - - - - 1, 2, 4, 7, 14, 28 and $1+2+4+7+14+28 = 56$,

496 has positive divisors $2^a \cdot 31^b$, $0 \le a \le 5$, $0 \le b \le 1$ and their sum is 2×496

A _Mersenne prime_ is a prime number of the form $p = 2^q - 1$ for some positive integer q. If p is prime, q itself must be a prime (if $q = hk$, then $2^q - 1$ is divisible by $2^h - 1$ and $2^k - 1$). $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$ are primes but $2^{11} - 1 = 2047 = 23 \times 89$ is not a prime.

If $p > 2$ is a Mersenne prime, then $p(p+1)/2$ is a perfect number. To see this, $p = 2^q - 1$ and $p + 1 = 2^q$, so with $n = p(p+1)/2 = p \cdot 2^{q-1}$,

$$d(n) = \left(\frac{p^2 - 1}{p - 1}\right)\left(\frac{2^q - 1}{2 - 1}\right)$$

$$= (p+1)(2^q - 1)$$

$$= 2^q(2^q - 1) = 2n.$$

Euler proved that every _even_ perfect _number_ is of the type $n = p(p+1)/2$ with p a Mersenne prime. It is not known at present whether an odd perfect number exists. It is also not known whether an even number of perfect numbers exist.

We finish with some more examples

① Prove that the product of two consecutive positive integers is not a perfect square

(A <u>perfect square</u> is the square of an integer).

<u>Proof</u> Let x be a positive integer and let $y = x(x+1)$. Suppose $y = z^2$ where z is an integer. Note that $\gcd(x, x+1) = 1$, so any prime dividing x cannot divide $x+1$ and vice versa. By unique factorization $z = z_1 z_2$ where z_1, z_2 are positive integers with $x = z_1^2$ and $x+1 = z_2^2$. But then $1 = z_2^2 - z_1^2 = (z_2 - z_1)(z_2 + z_1)$ and since $z_2 + z_1, z_2 - z_1$ are <u>positive</u> integers we must have $z_2 + z_1 = 1$, $z_2 - z_1 = 1$ and thus $z_1 = 0$ on subtraction, which is false. So the result is proved.

② Prove that the product of three consecutive positive integers is not a perfect square

<u>Proof</u>. Suppose x is a positive integer and $y = x(x+1)(x+2) = z^2$, where z is a positive integer. Note that $\gcd(x+1, x) = 1$ and $\gcd(x+1, x+2) = 1$, so $\gcd(x+1, x(x+2)) = 1$. By unique factorization, $z = z_1 z_2$ where z_1, z_2 are positive integers with $x+1 = z_1^2$ and $x(x+2) = z_2^2$. But then

$(x+1)^2 = x(x+2)+1 = z_2^2+1$ and thus $(x+1)^2 - z_2^2 = 1$. This gives a contradiction as in ①.

③ Prove that the product of four consecutive positive integers is not a perfect square.

Proof Let x be a positive integer and $y = x(x+1)(x+2)(x+3) = z^2$, for some positive integer z. Note that $y = x(x+3)(x+1)(x+2) = (x^2+3x)(x^2+3x+2) = ((x^2+3x)+1)^2 - 1$ and $(x^2+3x+1)^2 - z^2 = 1$, giving a contradiction as in ①.

④ Prove that the product of five consecutive positive integers is not a perfect square. (UKIMO Problem).

Proof. Let x be a positive integer and suppose that $y = x(x+1)(x+2)(x+3)(x+4) = z^2$ for some positive integer z.

Claim 1. At least one of the five numbers x, $x+1$, $x+2$, $x+3$, $x+4$ is coprime to 6.

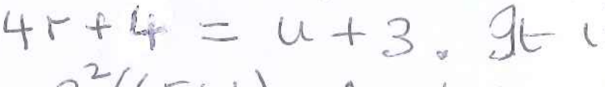
Proof of Claim 1: If x is even, then $x+1$ and $x+3$ are odd and at most one of them is divisible by 3. If x is odd, then $x+2$ is odd also and at most one of them is divisible by 3. The Claim follows.

Let u be a number satisfying Claim 1. We can write $u = 6m \pm 1$ for some positive integer m. Note that u must be coprime to the product of the other four numbers, since the least prime dividing u is at least 5 and u differs from the other four numbers by numbers in the set $\{1, -1, 2, -2, 3, -3, 4, -4\}$. So u is a perfect square, v^2, say, and $v = 6l \pm 1$ for some positive integer l. So $u = 36l^2 \pm 12l + 1 = 12l(3l \pm 1) + 1$ and $l(3l \pm 1)$ is even. So $u = 24r + 1$ for some positive integer r.

Claim 2. The numbers $x, x+1, x+2, x+3, x+4$ are $24r, 24r+1, 24r+2, 24r+3, 24r+4$.

Proof of this Claim. Notice that $24r-1 = u-2$ and it is coprime to 6, so if it was one of the numbers $x, x+1, x+2, x+3, x+4$, it would have to be a perfect square, w^2, say. But then $2 = u - w^2 = v^2 - w^2 = (v+w)(v-w)$ and one of the factors $v+w$, $v-w$ must be even. But $v+w = (v-w)+2w$, so both are even and their product cannot be 2.

The number $24r+5 = u+4$ is coprime to 6 and, if it was one of the numbers $x, x+1, x+2, x+3, x+4$, it would have to be a perfect square. But if $u+4 = y^2$, then $4 = y^2 - u = y^2 - v^2 = (y-v)(y+v)$ and y and v are both odd, so if $y-v = 2+4a$, where a is an integer, and $v = 2b+1$, then $y+v = 2+4a+2v = 4+4a+4b$ is divisible by 4. So either $y-v$ is divisible by 4 or $y+v$ is divisible by 4 and 8 divides $y^2-v^2 = 4$, which is impossible. So $24r+5$ is not in the list $x, x+1, x+2, x+3, x+4$, as claimed. So the result follows.



Finally, consider $24r+4 = u+3$. It is coprime to 3 and is $2^2(6r+1)$. Any prime dividing $6r+1$ does not divide $x, x+1, x+2, x+3$ and therefore it must be a perfect square. So $u+3 = f^2$, for some positive integer f and $f^2 - v^2 = 3$, $(f-v)(f+v) = 3$ and $f-v$, $f+v$ are positive integers, so $f-v = 1$, $f+v$ 3, $f = 2$, $v = 1$. So $u = 1$, which is impossible. So the result is true.

Exercises from First lecture

1. Prove that there is no prime numbers p such that p, $p+2$, $p+6$, $p+14$, $p+28$ are also prime.

2. Suppose that $p = 111\cdots1$ (k ones) is a prime number. Prove that k is prime.

3. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\cdots$, p_{2n} be the first $2n$ primes (in increasing order) and let $Q = A - B$ where A is the product of some of numbers $p_1, p_2, \cdots, p_{2n}$ and B the product of the rest. Proove that $|Q| \geq p_{2n} + 2$, if $|Q| \neq 1$.

4. Prove that $(7+2\sqrt{5})^{1/3} + (7-2\sqrt{5})^{1/3}$ is not rational.

5. Let p, q, r be primes. Prove that

$$\sqrt{p} + \sqrt{q} + \sqrt{r}$$

is not a rational number.

6. Let p be a prime number. Prove that

$$p^4 - p^2 + 1$$

is not a perfect square.

Solutions to the Exercises given in the Number Theory lecture of January 31 2015

1. Suppose $p, p+2, p+6, p+14, p+28$ are all prime numbers. We can write $p = 5q + r$ where q, r are integers and $0 \le r < 5$, $q \ge 0$.

If $r = 1$, $p+14 = 5q+15 = 5(q+3)$, so $p+14$ is divisible by 5 and $p+14 > 5$, so $p+14$ is not prime.

If $r = 2$, $p+28 = 5q+30 = 5(q+6)$ and $p+28$ is not prime.

If $r = 3$, then $p+2 = 5q+5 = 5(q+1)$ and $p+2$ is not prime.

If $r = 4$, then $p+6 = 5q+10 = 5(q+2)$ and $p+6$ is not prime.

So $r = 0$ and thus $p = 5$. But then $p+28 = 33$ is not prime.

So no such p exists.

2. Suppose that $k = ab$ where $a > 1$ and $b > 1$ are integers. Then $p = \underbrace{111\cdots 11}_{ab} = A(1+10^{a}+\cdots+10^{a(b-1)})$ and $A = 111\cdots1$ (a 'ones'), so p is not prime.

[Even if the number of ones k in forming p is prime, p need not be prime, for example $111 = 3 \times 37$].

3. The condition that $|Q| \neq 1$ should have been included in the question. When $n=1$, $p_1 = 2$, $p_2 = 3$ and taking $A = p_2$, $B = p_1$, we get $Q = 1$.

Assuming $|Q| \neq 1$, note $Q \neq 0$ by unique factorization So $|Q| > 1$. Let q be a prime dividing $|Q|$. If $q = p_j$ for some $j \leq 2n$, then q must divide A or B (since we split the primes $p_1, \cdots, p_{2n}$ into two (disjoint) sets in forming A and B. But q cannot divide both A and B, since the factorizations of A and B involve no common primes. So q does not divide Q. Hence q is a prime greater than p_{2n}. Now p_{2n} is an odd prime and the next prime p_{2n+1} must be at least $p_{2n}+2$. So

$$|Q| \geq q \geq p_{2n}+2.$$

4. Let $\alpha = (7+2\sqrt{5})^{1/3} + (7-2\sqrt{5})^{1/3}$. Then $\alpha^3 = (7+2\sqrt{5}) + 3\left((7+2\sqrt{5})(7-2\sqrt{5})\right)^{1/3}\left((7+2\sqrt{5})^{1/3} + (7-2\sqrt{5})^{1/3}\right) + 7 - 2\sqrt{5} = 3(\sqrt{29})^{1/3}\alpha + 14$. Suppose α is rational. Then so is $(\alpha^3 - 14)/(3\alpha) = (\sqrt{29})^{1/3}$ and thus so is $\left((\sqrt{29})^{1/3}\right)^3 = \sqrt{29}$. But this is impossible since we proved that for a positive integer n, $\sqrt{n}$ is irrational unless n is a perfect square, and 29 is not a perfect square.

5. Let $\beta = \sqrt{p} + \sqrt{q} + \sqrt{r}$. Suppose β is rational.

Now $\beta - \sqrt{p} = \sqrt{q} + \sqrt{r}$ and, squaring, we get

$$p + \beta^2 - 2\beta\sqrt{p} = q + r + 2\sqrt{qr}$$

Hence, since β^2, q and r are rational

$$\gamma = (2\sqrt{qr} + 2\beta\sqrt{p})/2 = \sqrt{qr} + \beta\sqrt{p}$$

is rational.

So $\gamma^2 = qr + \beta^2 p + 2\beta\sqrt{pqr}$ is rational

and thus $\sqrt{pqr} = \dfrac{\gamma^2 - qr - \beta^2 p}{2\beta}$ is rational

(since qr, $\beta^2 p$, $1/\beta$ are rational.

But $\sqrt{pqr}$ is rational only if pqr is a perfect square and this is impossible as it has three prime factors, and it would have to be an even number if it was a perfect square. This contradiction implies that β is not rational.

6. Let $\alpha = p^4 - p^2 + 1$ and suppose that $\alpha = q^2$ for a positive integer q. Then

$q^2 - 1 = p^4 - p^2$, that is

$$(q-1)(q+1) = p^2(p^2 - 1).$$

If a prime r divides $q-1$ and $q+1$, it must divide $-(q-1)+(q+1) = 2$. If $p = 2$, $\alpha = 13$ is not a square. So $p \neq 2$. So p^2 divides $q+1$ or $q-1$. Since $p^2 - 1 < p^2$, p^2 must divide $q+1$ and then $q+1 = kp^2$ and $q - 1 = kp^2 - 2$. So $p^2(p^2-1) = kp^2(kp^2-2)$, $k(kp^2-2) = p^2 - 1$, $k = (p^2-1)/(kp^2-2) < 1$ if $k > 1$, so $k = 1$ and this is impossible.