2001 Winter Camp

1 Division

The Division Algorithm *Let a and b be positive integers, $b \geq a$. Then there exist integers q, r satisfying $q \geq 1$ and $0 \leq r < a$ such that*

$$b = qa + 1.$$

Consequence *The greatest common divisor of a and b is the* **smallest** *combination of a and b.*

Example 1 (AIME 1985) The numbers in the sequence

$$101, 104, 109, 116, \cdots$$

are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \cdots$. For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.

Steps of the Solution

Start-Up Try some *small cases* and think about the problem. Trying some small cases for n may lead you to think that $d_n = 1$ for all n since the first numbers in our list are all relatively prime. The trick is *generalize the problem* first. What is so special about 100 in the definition of a_n. Maybe that it is 10^2. We will remember that and first replace it by $a_n = u + n^2$. Lets now make a table of a_n for different values of u:

u	a_1	a_2	a_3	a_4	a_5	a_6	a_7
1	2	**5**	**10**	17	26	37	50
2	3	6	11	**18**	**27**	38	51
3	4	7	12	19	28	**39**	**52**

The numbers in boldface are the pairs of numbers which have the highest GCD among the first 7 terms in the sequence. We are *looking for a pattern*. We see: when $u = 1$, the highest GCD is obtained by a_2 and a_3 and it is 5; when $u = 2$, the highest GCD is obtained by a_4 and a_5 and it is 9, when $u = 3$, it is obtained by a_6 and a_7 and its value is 13. We can make the following *conjecture*:

In general, for any fixed positive integer u, the numbers a_{2u} and a_{2u+1} have a GCD of $4u + 1$ and this is the largest GCD of consecutive numbers in the sequence.

Plan The Proof What are the different parts of the conjecture that we need to prove? (a) $4u+1$ divides a_{2u} and a_{2u+1}; (b) $4u+1$ is the *greatest* common factor of a_{2u} and a_{2u+1}; (c) $4u+1$ is the greatest possible GCD for *any pair of consecutive terms* in the sequence.

Part (a) Do some algebra:

$$a_{2u} = u + (2u)^2 = 4u^2 + u = u(4u+1)$$

and

$$a_{2u+1} = u+(2u+1)^2 = 4u^2+4u+1+u = 4u^2+5u+1 = (4u+1)(u+1)$$

So a_{2u} and a_{2u+1} share the common factor $4u+1$. (If you didn't see that last factorization, you can always find it using long division.)

Part (b) We saw that $a_{2u} = u(4u+1)$ and $a_{2u+1} = (u+1)(4u+1)$. Note that $(u, u+1) = 1$ (consecutive numbers are relatively prime), so

$$GCD(a_{2u}, a_{2u+1}) = 4u+1.$$

Part (c) According to the consequence of the division algorithm mentioned above it is sufficient to show that for any u and any n we can make a linear combination of $a_n = u+n^2$ and $a_{n+1} = u+(n+1)^2$ which is equal to $4u+1$. (This implies that all GCD's of pairs of consecutive numbers are factors of $4u+1$.) To make the proof more readable, make the following abbreviations:

$$a := a_n = u+n^2,\ b := a_{n+1} = u+(n+1)^2,\ g := (a,b).$$

Now we explore linear combinations of a and b with the hope of getting $4u+1$. They both contain n^2, so let us take

$$b - a = 2n+1. \tag{1}$$

How could we get rid of the n? Note that for the purpose of calculating the GCD, n is a constant. Since $a = u+n^2$, let us build the n^2 term. We have

$$n(b-q) = 2n^2+n,\ 2a = 2u+2n^2,$$

and thus

$$2 - n(b-a) = 2u-n. \tag{2}$$

Combining (1) and (2) gives:

$$2(2a - n(b-a)) + (b-a) = 2(2u-n) + (2n+1) = 4u+1.$$

So we have constructed a linear combination of a and b (specifically, $(3+2n)a+(1-2n)b$) that is equal to $4u+1$. Thus $g|(4u+1)$ no matter what n equals. Since this value had already been achieved, we conclude that $4u+1$ is the largest possible GCD of two consecutive terms.

Conclusion In the problem we are discussing we have that $u = 100$, so we conclude that the largest value for d_n is 401.

2 Congruences and Diophantine Equations

A *Diophantine Equation* is an equation whose variables only assume integral values. In this section we will review the general strategy and some tactics to deal with diophantine equations.

General Strategy Given a diophantine equation, there are four questions to ask yourself:

1. *Is the problem in 'simple' form?* Divide out common factors, and assume that the variables have no common factors.

2. *Do there exist solutions?* Sometimes you cannot solve the equation, but you can show that a solutions exist.

3. *Are there no solutions?* This is an important question. It may be rather easy to prove that an equation has no solutions!

4. *Can we find all solutions?* Once you have found one solution, try to understand how you can generate more solutions. It may still be quite tricky to prove that you have found all solutions.

Some Tactics The most important tactics for diophantine equations are *factorization, filtering mod n (especially parity) and GCD analysis*, but some examples below will also show the use of inequalities and comparison of exponents of primes in PPF's (powers of primes factorizations). We will use the following notation: $p^t||n$ means that t is the greatest exponent of p which divides n. For example, $3^2||360$.

Factoring is a tactic which can be used to find solutions. Here are some examples:

Example 2 (AIME 1986) What is the largest integer n for which $n^3 + 100$ is divisible by $n + 10$?

Example 3 Find all right triangles with integer sides such that the area and perimeter are equal.

Filtering mod n can be used to show that no solutions exist or that all solutions need to be of a particular form:

Example 4 Find all solutions to the diophantine equation $x^2 + y^2 = 1000003$.

Here is a problem for which the solution uses several tactics, but in a more complicated way. We will see how our tactics don't completely solve the problem, but the partial solutions point us to the correct solutions, which is rather surprising...

Example 5 (Putnam 1992) For a given positive integer m, find all triples (n, x, y) of positive integers, with n relatively prime to m, which satisfy

$$(x^2 + y^2)^m = (xy)^n.$$

Solution The most intimidating part of this problem are the exponents m and n. But the shape of the equation is asking for the use of the AM-GM inequality. This can be applied to eliminate some possibilities for the exponents. By AM-GM we have:

$$x^2 + y^2 \geq 2xy,$$

so

$$(xy)^n = (x^2 + y^2)^m \geq (2xy)^m = 2^m (xy)^m,$$

so we can conclude that $n > m$.

Let us look at some small examples. Start with $m = 1$, $n = 2$. Then the equation becomes

$$x^2 + y^2 = x^2 y^2.$$

Adding 1 to both sides and factoring gives

$$(x^2 - 1)(y^2 - 1) = 1,$$

which has no positive integer solutions. Unfortunately this technique can not be used in all cases. Our next example is $m = 3$, $n = 4$. Then the equation is

$$(x^2 + y^2)^3 = (xy)^4. \tag{3}$$

Factoring won't help us here, so try parity analysis, i.e. mod 2 filtering. There are four cases to consider, and it turns out that both x and y must be even. So we may write them as $x = 2a$ and $y = 2b$. After simplifying the equation becomes

$$(a^2 + b^2)^3 = 4(ab)^4.$$

We can apply parity once more to the variables a and b. They obviously can't be of opposite parity since the right hand side of the equation is even. But they can not be odd either: in that case the left hand side would be the cube of an even number (so it would have a factor 8), but the right hand side would be 4 times an odd number, which leads to a contradiction. We conclude that both a and b must be even. Writing $a = 2u$ and $b = 2v$ gives us

$$(u^2 + v^2)^3 = 16(uv)^4.$$

We could continue our parity analysis for this new equation, but rather than doing that, we will return to equation (3) and consider the powers of 2 in the PPF's of x and y. let r and s be the greatest exponents of 2 that divide x and y respectively. We write $x = 2^r \cdot a$ and $y = 2^s \cdots b$, where a and b are odd numbers, and r and s are positive by our first parity argument. There are two cases:

1. $r \neq s$, without loss of generality assume $r < s$. We can write (3) as

   $$(2^{2r}a^2 + 2^{2s}b^2)^3 = 2^{4r+4s}a^4b^4,$$

   and after dividing by the common factor 2^{6r}, we get

   $$(a^2 + 2^{2r-2s}b^2)^3 = 2^{4s-2r}a^4b^4.$$

   Notice that the exponent $4s - 2r$ is (strictly) positive, making the right hand side even. However, the left hand side is the cube of an odd number, which is odd. We conclude that there can not be any solutions.

2. $r = s$, in this case (3) becomes

$$(a^2 + b^2)^3 = 2^{2r}a^4b^4.$$

Both sides are even, but an analysis of the powers of 2 in both sides will lead us to a contradiction. Since a and b are both odd, we have that $a^2 \equiv b^2 \equiv 1(\text{mod } 4)$, so $a^2 + b^2 \equiv 2(mboxmod4)$. This means that $2^1||a^2+b^2$. Consequently, $2^3||(a^2+b^2)^3$. On the other hand, $2^{2r}||2^{2r}a^4b^4$, where r is a positive integer. Now it is impossible for $2r$ to be equal to 3. We conclude that also in this case there can not be any solutions.

We will now try to tackle the general case by comparing powers of 2. The small cases seem to indicate that there are no solutions, but there may be surprises. Consider the equation $(x^2 + y^2)^m = (xy)^n$. We know that $n > m$ and we can use the parity argument to show that both x and y need to be even. Let $2^r||x$ and $2^s||y$, as before. We consider the two cases:

1. $r < s$, then $2^{rm}||(x^2+y^2)^m$ and $2^{nr+ns}||(xy)^n$. This implies that $2rm = nr + ns$, but $nr + ns > 2rn > 2rm$, so we have a contradiction. There are no solutions in this case.

2. $r = s$, then write $x = 2^r \cdot a$, $y = 2^s \cdot b$, where a and b are both odd. The equation becomes

$$(x^2 + y^2)^m = 2^{2rm}(a^2 + b^2)^m,$$

where $a^2+b^2 \equiv 2(\text{mod } 4)$ as before and consequently $2^{2rm+m}||(x^2+y^2)^m$. Since $2^{2nr}||(xy)^n$, we equate

$$2rm + m = 2rn,$$

, and this equation does have solutions! For example, if $m = 6$, then $r = 1$ and $n = 9$ work. This doesn't mean yet that the original equation has solutions in this case. We will need to investigate further.

From this argument it follows that the factors of 2 in the PPF's of x and y need to be the same. Now remember that parity was a special case of mod n filtering. We can try to repeat this argument for any prime p. In case 1 of the last argument, write $p^u||x$ and $p^v||y$. If we assume that $u < v$, we can conclude that $p^{2um}||(x^2 + y^2)m$ and $p^{nu+nv}||(xy)^n$, and this is impossible because $n > m$ and $v > u$. So we need again that $u = v$.

What do we conclude? Since the powers of all primes in the PPF's of x and y need to be the same, we have that that there are only possibly solutions to the equation if $x = y$. In that case the equation becomes

$$\left(2x^2\right)^m = \left(x^2\right)^n,$$

so $2^m x^{2m} = x^{2n}$, or $x^{2n-2m} = 2^m$. Thus $x = 2^t$, and we have $2nt - 2mt = m$, or

$$(2t+1)m = 2nt.$$

Finally, use the hypothesis that $n \perp m$. Also note that $2t+1 \perp 2t$, so the only way this equation can be true is if $n = 2t+1$ and $m = 2t$. And this finally produces infinitely many solutions. If $m = 2t$ and $n = m+1$, then it is easy to check that $x = y = 2^t$ indeed satisfies $(x^2+y^2)^m = (xy)^n$.

The argument above shows that these are the only solutions. This solution can be described in the following way: if m is odd, there are no solutions, and if m is even, there is a single solution

$$n = m+1, \ x = y = 2^{m/2}.$$

3 If you can count it...

We end these notes with an example to encourage you to keep your point of view flexible. The following problem looks as if it is a number theory problem, but it has a very nice combinatorial solution.

Example 6 Let $k \in \mathbb{N}$. Show that the product of k consecutive integers is divisible by $k!$.

4 More Problems

1. (USAMO 1972) Let $a, b \in \mathbb{N}$. Show that

$$\frac{[a,b,c]^2}{[a,b][c,b][c,a]} = (a,b,c)^2 (a,b)(b,c)(c,a),$$

where $[a,b] = \text{LCM}(a,b)$.

2. Show that
$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$$
can never be an integer.

3. (Russia, 1995) The sequence $a_1, a_2, \cdots$ of natural numbers satisfies
$$(a_i, a_j) = (i, j)$$
for all $i \neq j$. Prove that $a_i = i$ for all i.

4. (USAMO 1973) Show that the cube roots of three distinct prime numbers cannot be three terms (not necessarily consecutive) of an arithmetic progression.

5. If $x^3 + y^3 = z^3$, show that one of the three must be a multiple of 7.

6. Let $f(n)$ denote the sum of the digits of n.

   (a) For any integer n, prove that eventually the sequence
   $$f(n), f(f(n)), f(f(f(n))), \cdots$$
   will become constant. This constant value is called the *digital sum* of n.

   (b) prove that the digital sum of the product of two twin primes, other than 3 and 5, is 8. (Twin primes are primes that are consecutive odd numbers, such as 17 and 19.)

   (c) (IMO1975) Let $N = 4444^{4444}$. Find $f(f(f(n)))$, without a calculator.

7. (USAMO 1995) Let p be an odd prime. The sequence $(a_n)_{n\geq 0}$ is defined as follows: $a_0 = 0, a_1 = 1, \ldots, a_{p-2} = p-2$ and, for all $n \geq p-1$, a_n is the least integer greater than a_{n-1} that does not form an arithmetic sequence of length p with any of the preceeding terms. Prove that, for all n, a_n is the number obtained by writing n in base $p-1$ and reading the result base p.

8. (Putnam 1996) Suppose a, b, c, d are integers with $0 \leq a \leq b \leq 99$, $0 \leq c \leq d \leq 99$. For any integer i, let $n_i = 101i + 1002^i$. Show that if $n_a + n_b$ is congruent to $n_c + n_d$ mod 10100, then $a = c$ and $b = d$.

9. (Greece, 1995) Find all positive integers n for which $-5^4 + 5^5 + 5^n$ is a perfect square. Do the same for $2^4 + 2^7 + 2^n$.

10. (United Kingdom, 1995) Find all triples of positive integers a, b, c) such that
$$\left(1+\frac{1}{a}\right)\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right) = 2.$$

11. Show that there is exactly one integer n such that $2^8 + 2^{11} + 2^n$ is a perfect square.

12. Find the number of ordered pairs of positive integers (x, y) that satisfy
$$\frac{xy}{x+y} = n.$$

13. (USAMO 1979) Find all non-negative integral solutions $(n_1, n_2, \ldots, n_{14})$ to
$$n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1,599.$$

14. Find all positive integer solutions to $abc - 2 = a + b + c$.

15. (Germany, 1995) Find all pairs of nonnegative integers (x, y) such that $x^3 + 8x^2 - 6x + 8 = y^3$.

16. (India, 1995) Find all positive integers x, y such that $7^x - 3^y = 4$.

17. (India, 1996) Find all positive integer solutions x, y, z, p with p a prime, of the equation $x^p + y^p = p^z$.

18. Show that $(a+b)^p \equiv a^p + b^p (\text{mod } p)$ for any prime p.

19. (Putnam 1983) How many positive integers n are there such that n is an exact divisor of at leats one of the numbers 10^{40}, 20^{30}?

20. (Kiran Kedlaya) Let p be an odd prime and $P(x)$ a polynomial of degree at most $p-2$.

    (a) Prove that if P has integer coefficients, then $P(n) + P(n+1) + \cdots + P(n+p-1)$ is an integer divisible by p for every integer n.

    (b) If $P(n) + P(n+1) + \cdots + P(n+p-1)$ is an integer divisible by p for every integer n, must P have integer coefficients?

21. (IMO1972) Let m and n be arbitrary non-negative integers. Show that

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

is an integer.

22. Find all integer solutions to

$$x^2 + y^2 + z^2 = 2xyz.$$

23. Show that

$$\binom{n}{1}, \binom{n}{2}, \cdots, \binom{n}{n-1}$$

are all even if and only if n is a power of 2.

24. (IMO1974) Prove that the number

$$\sum_{k=0}^{n} \binom{2n+1}{2k+1} 2^{3k}$$

is not divisible by 5 for any integer $n \geq 0$.

25. (Romania, 1995) Let $f: \mathbb{N} - \{0, 1\} \to \mathbb{N}$ be the function defined by

$$f(n) = \text{LCM}[1, 2, \cdots, n].$$

(a) Prove that for all n, $n \geq 2$, there exist n consecutive numbers for which f is constant.

(b) Find the greatest number of elements of a set of consecutive integers on which f is strictly increasing, and determine all sets for which this maximum is realized.