Olympiad NT Theorem Collection

Technique 1:

In number theory problems, if you see some thing of the sort: $\frac{1}{a}+\frac{1}{b}=\frac{1}{c}$ where a, b, c are integers, it is helpful to replace a by $c+x$ and b by $c+y$

Problem to do using this:

For any positive integer n, let $S(n)$ denote the number of ordered pair (x, y) of positive integers for which $\frac{1}{x}+\frac{1}{y}=\frac{1}{n}$. (for instance, $S(2)=3$). Determine the set of positive integers n for which $S(n)=5$ -Indian National MO,1991

Solution:

Putting $x=n+a$ and $y=n+b$, we get $n^2=ab$. If n is prime, then $S(n)=3$. If $n=pq$, where p and q are primes then $S(n)>5$ $\therefore S(n)=5$ iff $n=p^2$, where p is prime when $(a,b)=(1,p^4),(p^4,1),(1,p^3),(p^3,1),(p^2,p^2)$

Technique 2:(Extremal Principle)

In extreme conditions use Extremal Principle!!!
This technically means looking at the maximal or minimal quantities,values or elements

Problems to do with this:

Find all positive integers x, y such that $2^x-1=xy$

Another very good problem on extremal principle:

Of $2n+3$ points of a plane, no 3 are collinear and no 4 are concyclic. Prove that we can choose 3 of these and draw a circle through them, so that exactly n lie outside and n inside(ChNO)

Technique 3:(Bertrand's Postulate)

For every positive integer n, there exists a prime $p$such that $n \leq p \leq 2n$. Use this when somewhere you need to check the existence of a prime in sequence/sub-sequence

Wikipedia:

"Bertrand's postulate (actually a theorem) states that if n > 3 is an integer, then there always exists at least one prime number p with n < p < 2n − 2. A weaker but more elegant formulation is: for every n > 1 there is always at least one prime p such that n < p < 2n."

Problem to do using this:

Prove that $n!$ is not a square

Technique 4:

Finding the residues of the factor modulo some integer.

Problem to do with this:

Well known but still as an example:
Prove that the divisors of x^2+1 are of the form $4k+1$ or is 2.

Technique 5:

For factorization one can also use roots of unity:
For example $a^{3k+2}+a^{3m+1}+a^{3n}$ is divisible by a^2+a+1 as In the original expression if we put $a=\omega$ we get $\omega^{3k+2}+\omega^{3m+1}+\omega^{3n}=\omega^2+\omega+1$ where ω is the cube root of unity. (We can also use the other roots of unity in the same way).

Problem:

Prove 1280000401 is composite. (IIM 1993)
Observe that $1280000401=2^7+2^2+2^0$ which is of the form a^7+a^2+1 hence is divisible by a^2+a+1. Or in this case 421 where $a=2$.

Technique/Advice 6:

When the problem involves number theoritic functions like $[x], \phi(x)$, etc., dribbling with expression or factoring won't help much. You have to use their properties.
Here I will give some of the main properties of $[x]$:
Firstly, $x-[x]=\{x\}$, which called fraction part of x
And 2nd: $-[-x]$ is the least integer $\geq x$
I have attached the properties:

$[x] \leqslant x < [x] + 1$, $x - 1 < [x] \leqslant x$, $0 \leqslant x - [x] < 1$.
$[x] = \Sigma_{1 \leqslant i \leqslant x} 1$ *if* $x \geqslant 0$.
$[x + m] = [x] + m$ *if m is an integer.*
$[x] + [y] \leqslant [x + y] \leqslant [x] + [y] + 1$.
$[x] + [-x] = \begin{cases} 0 \text{ if } x \text{ is an integer,} \\ -1 \text{ otherwise.} \end{cases}$
$\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$ *if m is a positive integer.*
$-[-x]$ *is the least integer* $\geqslant x$.
$[x + \frac{1}{2}]$ *is the nearest integer to x. If two integers are equally near to x, it is the larger of the two.*
$-[-x + \frac{1}{2}]$ *is the nearest integer to x. If two integers are equally near to x, it is the smaller of the two.*
If n and a are positive integers, $[n/a]$ is the number of integers among $1, 2, 3, \cdots, n$ *that are divisible by a.*

Problem to do using this:

Define $q(n) = [\frac{n}{[\sqrt{n}]}]$ for $n = 1, 2, 3 \ldots$. Determine all positive integers n for which $a_n > a_{n+1}$ (British MO, 1996)

For each integer $n \geq 1$, define $a_n = [\frac{n}{[\sqrt{n}]}]$. Find the number of all n in the set $1, 2, 3, \ldots, 2010$ for which $a_n > a_{n+1}$ (India Regional MO,2010)
Well, "*History repeats itself, historians repeat each other*"- Philip Guedalla

Technique 7:(Infinite Descent)

The statement states that any non-zero integer is not divisible by any prime infinitely many primes.
In other words if $\exists$a prime p and ineteger n such that $n = p^{\alpha} m$and $\alpha = \infty \iff n = 0$.

Problem to do using this:

1. Prove that $\sqrt{2}$ is irrational.
2. Find all $x, y \in \mathbb{Z}^2$such that $x^2 + y^2 = x^2 y^2$
3. Solve in integers x, y, z such that $x^3 + 2y^3 = 4z^3$

Solution of 2 in another way:

$x^2 + y^2 - x^2y^2 - 1 = -1 \implies x^2(1 - y^2) - (1 - y^2) = -1 \implies (x^2 - 1)(y^2 - 1) = 1$
Then
Case 1:

$x^2-1=1$ and $y^2-1=1 \implies no$ integer solution
Case 2:
$x^2-1=-1$ and $y^2-1=-1 \implies \boxed{(x;y)=(0;0)}$
Better to follow infinite descent... At least one of x, y have to be even implying the other is even too..
Then we have the required descent...

Technique 8:(Inequalities)

Showing the RHS is far too large than LHS is a very powerful instrument.

Corollary:(Very useful)

Integers m, n satisfy $m \mid n \iff |m| \leq |n|$

Problem to do with this:

Find all positive integers n such that $n-\tau(n) \mid n$

Hint:

Just use $\tau(n) \leq 2\sqrt{n}$

Technique 9:

Generating polynomials by working in $\mathbb{Z}_p$.
For example: In $\mathbb{Z}_p$, $p$is a prime
We get $x^{p-1}-1=0$by Fermat's Theorem $\forall x \in \mathbb{Z}_p/\{0\}$

So, $x^{p-1}-1=(x-1)(x-2)\cdots(x-p+1)$

Problem to do with this:

In all these problems we asume p is any prime;

- $\binom{2p}{p} \equiv 2 \pmod{p^3}$
- $\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3} **$

$**$In this Problem you need the help of other Theorem's such as Wolstenholme's Theorem, e.t.c.

Technique 10:(Wolstenholme's Theorem)

If $1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p-1}=\frac{A}{B}$, where p is prime then $p^2|A$
In fact,

$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}$ is another way of stating the theorem. If $\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^4}$ then p is Wolstenholme prime.

(The second one just implies from the first one)
Reason:
$$\binom{ap}{bp} - \binom{a}{b} \equiv a(a-1)\binom{a-2}{b-1}\left(\binom{2p}{p} - 2\right) \pmod{p^3}$$

Problem to do with this:

Let p be a prime congruent to 1 modulo 4, let $\sum_{k=1}^{p-1}(-1)^{k-1}\frac{1}{k} = \frac{A}{B}$, and $\sum_{k=1}^{\frac{p-1}{4}}\frac{1}{k} = \frac{C}{D}$, here A, B, C, D are all integers , and $gcd(A, B) = 1$, $gcd(C.D) = 1$. Prove that p divides C iff p divides A

Small Hint:

Use Wolstenholme's Theorem

Big Hint:

$$\sum_{k=1}^{p-1}(-1)^{k-1}\frac{1}{k} = \sum_{k=1}^{p-1}\frac{1}{k} - \sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k}$$

By Wolstenholme's Theorem, the numerator of the two expression on the RHS is divisible by p. Thus p always divides A.

Thus we have to show p always divides C.

Technique 11:(Multiplicative Inverse)

If $\gcd(b, m) = 1, \quad b \mid a$

Then $\frac{a}{b} \equiv ab^{-1} \pmod{m}$

Problem to do with this:

•$(p-1)! \equiv -1 \pmod{p}$

•$1 + \frac{1}{2} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}$

(In the second problem p > 5)

Technique 12:

Be innovative, think geometrically or combinatorially. Given a expression think whether it is in the form of some length/area/angle. This helps in solving diophantine equations sometimes. Also given an expression, think whether it can be interpreted combinatorially. This directly shows the expression is a positive integer.

Problem to do with this:

1. Prove that $\frac{(2m!)(2n!)}{m!n!(m+n)!}$ is always an integer. (IMO 72) [Think combinatorially]
2. Show that there does not exist an integer k such that the equation:
$x^2y^2 = k^2(x+y+z)(x+y-z)(y+z-x)(z+x-y)$
has positive integral solution. [Think geometrically]

Solution of 2:

If x, y, z do not satisfy triangle inequality, exactly one term on the RHS is negative, but LHS is a square, so this can't happen. So let x, y, z be sides of a triangle, giving $xy = 4k(Area) = 2kxy \sin Z$, so $\sin Z = 1/2k$ is rational. But $z^2 = x^2 + y^2 - 2xycosZ$, so cos Z $= \sqrt{4k^2-1}/2k$ must be rational. Then $(2k)^2 - 1$ is a square so $2k = 1$, contradiction since k is supposed to be an integer. So no solutions.

As for the other one, it seems like the usual $v_p(n!)$ method with some inequality of floors is more efficient than finding a combinatorial interpretation :/

Technique 13:(Lucas's Theorem)

Write m, n in base p(for p prime) as $m_0 + m_1p + m_2p^2 + \ldots + m_kp^k$ and $n_0 + n_1p + n_2p^2 + \ldots + n_kp^k$ respectively. Then $\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod p$.

Use this in problems involving binomial coefficients mod p.

Lucas's Theorem itself (as well as Wolstenholme, Wilson, and lots of other useful stuff) can be proven in a very simple way using technique 9 and the fact that factorization is unique in polynomials mod p.

Problem to do with this:

Prove that in any row of Pascal's Triangle, the number of odd coefficients is a power of 2.

Can someone give a brief explanation of how UFDs (and related concepts), like $\mathbb{Z}[\sqrt{3}]$, work in solving Olympiad NT problems?

Example problem:

Find all integer solutions to the equation $x^2+2=y^3$.

Solution:

To solve this problem we work in $\mathbb{Z}[\sqrt{-2}]$.
Clearly, y is odd.
We factor the left side as $(x+\sqrt{-2})(x-\sqrt{-2})$. Suppose p is a prime in $\mathbb{Z}[\sqrt{-2}]$ that divides both $x+\sqrt{-2}$ and $x-\sqrt{-2}$. Then p also divides $2\sqrt{-2}=-\sqrt{-2}^3$, so p $=\pm\sqrt{-2}$. However, p must also divide y^3, a contradiction. thus, $x+\sqrt{-2}$ and $x-\sqrt{-2}$ are coprime. Thus, $x+\sqrt{-2}=(a+b\sqrt{-2})^3$. Solving the equation for a and b gives $x=\pm 5, y=3$.

This problem uses unique factorization in $\mathbb{Z}[\sqrt{-2}]$.

powerful technique:

A very powerful technique involving proving polynomials irreducible in $\mathbb{Z}[x]$ is reducing the polynomial in mod p and working from there. Gabriel Dospinescu taught this strategy in Number theory at Awesomemath.

Example problem (generalization of chinese TST and IMO 1993)

$P\in\mathbb{Z}[x]$ is monic and has degree 2, and has no real roots. Furthermore, P(0) is squarefree. Prove that $P(x^n)$ is irreducible for all natural numbers n.

Solution:

Let $f=P(x^n)$. It is clear that for all n, f has no real roots. Let $f(x)=x^n+ax^{n-1}+q$. Let p be a prime that divides q. If we reduce f in $\mathbb{F}_p$, it becomes $x^n+ax^{n-1}=x^{n-1}(x+a)$.
Suppose f = gh, where $g,h\in\mathbb{Z}[x]$. WLOG, we have $g=x^k+pg_1(x)$ and $h=x^{n-k-1}(x+a)+ph_1(x)$, where g_1 and h_1 are integer polynomials. In the case that k = 0,

g is constant, a contradiction. If k = n - 1, then f must have an integer root, also a contradiction. Thus, 0 < k < n - 1. However, multiplying g and h and setting the product equal to f gives $p^2 g_1 h_1 = q$. However, $v_p(q) = 1$ since q is squarefree. Thus, f is irreducible.

This strategy can be applied to many problems, such as an IMO 1993, a China TST 1994, and a Romania TST 2006.
Thank you Gabriel for teaching me this most powerful technique for proving irreducibility.

(Erm, your statement also needs the constant term is not ± 1or else the prime doesn't exist. Furthermore, $f = x^{2n} + ax^n + q$, not $x^n + ax^{n-1} + q$...)

Technique 13:

Try introducing the following things in Diophantine equations:
1. If you find a variable(say a) is always greater than say b, substitute $a = b + k$. This might help to reduce the power.
2. Remember discriminant ≥ 0

Problem to do with this:

Solve the Diophantine equation: $x^3 - y^3 = xy + 61$.

Lemma:

Let x, y be integers and p be a prime of the form $4k + 3$. Then $p \mid x^2 + y^2 \Rightarrow p \mid x, y$.

Problem:

Find all pair of positive integers (x, y) for which
$$\frac{x^2 + y^2}{x - y}$$
is an integer which divides 1995.

(Source: Bulgaria 1995)

Lemma:

Let x, y be integers and p be a prime of the form $3k + 2$. Then $p \mid x^2 + xy + y^2 \Rightarrow p \mid x, y$.

Problem:

Prove that there are no nontrivial solutions to the Diophantine equation $x^2 + y^2 + z^2 = 6(xy + yz + zx)$.

Technique 14:

$m|n \Rightarrow V_p(m) \leq V_p(n)$ and Legendre formula $V_p(n!) = \sum_{r\geq 1}[\frac{n}{p^r}]$
with $[x]$ the floor function.

Problem to do with this:

show that : $\frac{(m+n)!}{m!n!}$ is always integer for all integers m and n .