0.1. Basic Num. Th. Techniques/Theorems/Terms.

Modular arithmetic, Chinese Remainder Theorem, Little Fermat, Euler, Wilson, totient, Euclidean algorithm, unique factorization, linear diophantine equations, Pythagorean triplets, Pell, infinite descent.

0.2. Putnam & Beyond Num. Th. Prob. for those with Less Time.

Putnam & Beyond Readings: Chapter 5, pages 245-279.

5.1.2 (Fermat’s Infinite Descent Principle). A basic technique. The first example is an easy one, but the reference to “the maximum modulus principle” may be unfamiliar to those who haven’t studied complex analysis. (Complex analytic functions always attain their maximum modulus on the boundary of their domains.)

706 is easy. 707 a bit harder. 708 is cute but not easy for all.

5.1.3 (The Greatest Integer Function). Discussion is amazing but may not be quick.

5.2.1 (Factorization and Divisibility). Examples 1 and 2 on page 253 are quick.

724 is quick. As is 725 . . . with the right observation.

5.2.2 (Prime Numbers). The first example is interesting but elaborate with an apparent typo in the centered equation just before the end.

The example at the bottom of page 255 is good and quick.

Polignac’s formula on page 257 is quite intuitive and easy to carry with you

733 is fairly easy.

744 good and systematic.

747 and 748 are interesting Polignac problems.
5.2.3 (Modular Arithmetic). Example 1 is quick and basic. Example 2 is interesting and may open some eyes; but will take more thought.

750, 751, and 752 relatively quick.

753 cute and quick with the right observation.

5.2.4 (Fermat’s Little Theorem). A very basic theorem. The proof is a little exotic but illustrates a powerful technique.

Example 1 page 262 relatively quick but tricky. Example 2 harder to come up with.

760 cute and quick. 761 quick - was on a recent practice Putnam.

762 first part easy and interesting. The application is harder, but quick.

5.2.5 (Wilson’s Theorem). A basic theorem with a quick proof.

The example is quite nice and quick.

769 is quick and cute. 770 is slick and quick.

771 is nice and famous. 772 is a good application.

5.2.6 (Euler’s Totient Function). Quite a fundamental function. The proposition is another basic result. Proofs based on $\phi(mn) = \phi(m)\phi(n)$ when $\gcd(m, n) = 1$ may be more accessible.

Euler’s theorem comes up a lot and two good proofs are given.

The first example is a good and quick application.

5.2.7 (The Chinese Remainder Theorem). Again fundamental. The proof is given in an interesting constructive form; can also be viewed as a byproduct of techniques for solving linear diophantine equations.

The example at the bottom of page 269 is amazing.

785 is a basic application. 786 is cute and in the end an easy Chinese Remainder Theorem Application. 787 is a good quick application.
0.3. A Few Interesting Problems.

(Solutions on next page.)

**Problem 1:** *(Putnam 1985 A4)* Define a sequence \( \{a_i\} \) by \( a_1 = 3 \) and \( a_{i+1} = 3^{a_i} \) for \( i \geq 1 \). Which integers between 00 and 99 inclusive occur as the last two digits in the decimal expansion of infinitely many \( a_i \)?

**Problem 2:** For how many integers \( n \) between 49 and 100 (inclusive) is the binomial coefficient \( \binom{n}{49} \) odd?

**Problem 3:** Show that the equation \( x^2 + y^2 + z^2 = 2xyz \) has no nontrivial solutions.

**Problem 4:** Find all integral solutions of \( x^2 - 3y^2 = 1 \).
0.4. Soln. to Num. Th. Problems on Previous Page.

Soln. to Problem 1:
We are interested in \(a_n \mod 100\). Note all of the \(a_n\) satisfy \(gcd(a_n, 100) = 1\).

Little Fermat says \(a^{p-1} \equiv 1 \mod p\) for a prime number \(p\) and \(a\) not divisible by \(p\). More generally, Euler’s theorem says if \(gcd(a, m) = 1\), \(a^{\phi(m)} \equiv 1 \mod m\) where \(\phi(m)\) is the number of residue classes mod \(m\) which are coprime to \(m\).

Also note \(\phi(ab) = \phi(a)\phi(b)\) when \(gcd(a, b) = 1\) and \(\phi(p^k) = p^k - p^{k-1}\) for \(p\) a prime.

So \(a_{i+1} \equiv 3^{a_i} \mod 100\) is determined by \(a_i \mod \phi(100)\) or \(a_i \mod 40\) since \(\phi(100) = \phi(5^2 \cdot 2^2) = \phi(5^2) \cdot \phi(2^2) = (5^2 - 5)(2^2 - 2) = 40\).

Then \(a_i \equiv 3^{a_{i-1}} \mod 40\) is determined by \(a_{i-1} \mod \phi(40)\) or \(a_{i-1} \mod 16\) since \(\phi(40) = \phi(2^3 \cdot 5) = \phi(2^3) \cdot \phi(5) = (2^3 - 2^2)(5 - 1) = 16\).

Continuing \(a_{i-1} \equiv 3^{a_{i-2}} \mod 16\) is determined by \(a_{i-2} \mod \phi(16)\) or \(a_{i-2} \mod 8\) since \(\phi(16) = 2^4 - 2^3 = 8\).

Continuing \(a_{i-2} \equiv 3^{a_{i-3}} \mod 8\) is determined by \(a_{i-3} \mod \phi(8)\) or \(a_{i-3} \mod 4\) since \(\phi(8) = 2^3 - 2^2 = 4\).

Continuing \(a_{i-3} \equiv 3^{a_{i-4}} \mod 4\) is determined by \(a_{i-4} \mod \phi(4)\) or \(a_{i-4} \mod 2\) since \(\phi(4) = 2^2 - 2 = 2\).

All \(a_{i-4}\) for \(i \geq 4\) are odd, so working backwards,

\[
\begin{align*}
a_{i-3} & \equiv \quad 3 \mod 4 \\
a_{i-2} & \equiv \quad 3^3 \mod 8 \equiv \quad 3 \mod 8 \\
a_{i-1} & \equiv \quad 3^3 \mod 16 \equiv \quad 11 \mod 16 \\
a_i & \equiv \quad 3^{11} \mod 40 \equiv \quad ((3^4)^2)(3^{3}) \mod 40 \equiv \quad (3^{3}) \mod 40 \equiv \quad 27 \mod 40 \\
a_{i+1} & \equiv \quad 3^{27} \mod 100 \equiv \quad ((3^6)^4)(3^{3}) \mod 100 \equiv \quad (729^4)(3^{3}) \mod 100 \equiv \quad 29 \cdot 87^3 \mod 100 \\
& \quad \text{and} \\
29 \cdot 87^3 \mod 100 & \equiv \quad 29(-13)^3 \mod 100 \equiv \quad 29 \cdot (169 \cdot -13) \mod 100 \\
& \equiv \quad 29(-2197) \mod 100 \equiv \quad 87 \mod 100.
\end{align*}
\]

So all but the first few terms end in 87.

Soln. to Problem 2:
First note that
\[
(x + y)^p = x^p + y^p \quad (\mod p)
\]
for a prime number \(p\) since \(\left( \begin{array}{c} p \\ a \end{array} \right) \equiv 0 \mod p\) when \(0 < a < p\). So also
\[
(x + y)^{p^k} = x^{p^k} + y^{p^k} \quad (\mod p).
\]
We can use this to establish
\[
\begin{align*}
\left( \begin{array}{c} b \\ a \end{array} \right) &= \Pi \left( \begin{array}{c} b_i \\ a_i \end{array} \right) \pmod{p} \\
\end{align*}
\]
where \( b = \Sigma b_i p^i \) and \( a = \Sigma a_i p^i \) give the base \( p \) expansions of \( a \) and \( b \).

This is seen by observing
\[
(x + y)^b \equiv (x + y)^{\Sigma_i b_i p^i} \equiv \Pi_i \left( x^{p^i} + y^{p^i} \right)^{b_i} \equiv \Pi_i \Sigma_k \left( \begin{array}{c} b_i \\ k \end{array} \right) \left( x^{kp^i} y^{(b_i-k)p^i} \right) \pmod{p}
\]
and comparing the coefficients of \( x^a y^{b-a} \).

Since \( 49 = 32 + 16 + 1 = 11001_2 \) and we are interested in \( n \leq 100 \), we first do the problem for \( n \leq 127 \). For the binomial coefficient to be odd, the 7 or less bit number \( n \) in base 2 must look like
\[
(0 \ or \ 1)11(0 \ or \ 1)(0 \ or \ 1)(0 \ or \ 1)12
\]
a total of \( 2^4 = 16 \) possibilities. Since \( 64 + 32 + 16 + 1 > 100 \), the eight possibilities whose 64 column is 1 are too big, and we have the remaining eight possibilities where the binomial coefficient is odd.

**Soln. to Problem 3:**
First, let \((x, y, z)\) be a nontrivial solution of
\[
(*) \ x^2 + y^2 + z^2 = 2xyz.
\]
Mod 4, squares are 0 or 1 and \( 2xyz \) is 0 unless all of \( x, y, z \) are odd. So any nontrivial solution consists entirely of even integers.

Writing \( x = 2\bar{x}, y = 2\bar{y}, z = 2\bar{z} \), we have a nontrivial solution \((\bar{x}, \bar{y}, \bar{z})\) to
\[
x^2 + y^2 + z^2 = 4xyz.
\]

But then the same argument modulo 4 shows that \( \bar{x}, \bar{y}, \bar{z} \) must all be even and we can repeat.

Motivated by this, we use Fermat’s method of descent to show there are no nontrivial solutions. Let \((\bar{x}, \bar{y}, \bar{z})\) be a “minimal” nontrivial solution to
\[
(**) \ x^2 + y^2 + z^2 = 2^kxyz.
\]
for some positive integer \( k \) where by minimal we mean having the smallest positive value of \( x \) among all nontrivial solutions to \((**)\) regardless of the positive value of \( k \). The above argument modulo 4 shows that all of \( \bar{x}, \bar{y}, \bar{z} \) are even. But then \((\bar{x}/2, \bar{y}/2, \bar{z}/2)\) would solve \((**)\) with \( k \) increased by 1 contradicting the assumption that \((\bar{x}, \bar{y}, \bar{z})\) was a solution minimal in \( x \) value.

So no nontrivial solutions to \((**)\) exist.

**Soln. to Problem 4:**
This equation is called Pell’s equation and will work similarly if 3 is replaced by any other square-free positive integer. Since \((x, y)\) a solution implies \((-x, -y)\) is also (and there are no solutions with \(x = 0\)), we just need to think about solutions with \(x > 0\).

The equation may be rewritten as

\[
(\ast) \left( x - y\sqrt{3} \right) \left( x + y\sqrt{3} \right) = 1
\]

or \(z\overline{z} = 1\) where \(z = x + y\sqrt{3}\) (with \(x, y \in \mathbb{Z}\)) and \(\overline{z} = x - y\sqrt{3}\). (Note that the product of two numbers of the form \(x + y\sqrt{3}\) with \(x, y\) integers can be simplified into a number of the same form.)

Let \(S = \{x + y\sqrt{3} : x, y \in \mathbb{Z}, x > 0, \text{ and } (x, y) \text{ solves } (\ast)\}\). Then \(ab = \overline{ab}\) means \(z_1, z_2 \in S \Rightarrow z_1z_2 \in S\).

Also \(z \in S \Rightarrow \frac{1}{z} \in S\) as well since \(z\overline{z} = 1\) and \(\frac{1}{z} = \overline{z}\) for elements of \(S\).

Thus the product and quotient of elements of \(S\) are also in \(S\).

When an element of \(S\) \(x + y\sqrt{3}\) is greater than 1, \(x - y\sqrt{3} < 1\) since their product is 1. Thus the set of solutions \(S\) with \(x > 0\) is partitioned into two subsets

\[
S^+ = \{x + y\sqrt{3} \in S : x > 0 \text{ and } y \geq 0\}
\]

\[
S^- = \{x - y\sqrt{3} \in S : x > 0 \text{ and } y > 0\}.
\]

\(S^+\) consists of those elements of \(S\) bigger than or equal to 1; \(S^-\) those elements between 0 and 1.

Now let \(u_0\) be the smallest element of \(S^+\) bigger than 1. We claim all solutions of \((\ast)\) with \(x > 0\) (interpreted as elements of \(S\)) are whole number powers \(u_0^k\) of \(u_0\).

For if \(u = x + y\sqrt{3}\) is any other positive solution with \(x > 0\), since \(u_0 > 1\), there is a unique integer \(k\) so that

\[
u_0^k < u < u_0^{k+1}.
\]

Multiplication by \(u_0^{-k}\) gives a solution with

\[
1 < u_0^{-k} < u_0.
\]

But \(u_0^{-k}\) being a solution bigger than 1 forces it to be in \(S^+\) contradicting the assumption that \(u_0\) was the smallest element bigger than 1.

So no additional solution \(u\) exists.

In our case of \(x^2 - 3y^2 = 1\), \(u_0 = 2 + \sqrt{3}\) by inspection. Hence all solutions of \((\ast)\) interpreted as numbers \(z = x + y\sqrt{3}\) are simply \(\pm u_0^k\) for \(k \in \mathbb{Z}\).