PROBLEM SOLVING 101
No. 2
Shawn Godin

This month, we will look at assignment #3 from the course C & O 380 that I took back in 1986. You can check out the first two assignments in earlier issues [2017: 43(4), p. 151 - 153] and [2017: 43(8), p. 344 - 346].

In the Ross Honsberger Commemorative issue, I presented the problems, and a solution to problem #5, from Assignment #1 of the course C & O 380 that I took with Professor Honsberger back in 1986 (Crux 43(4), p. 151–153). This month, we will look at Assignment #2.

<table>
<thead>
<tr>
<th>C&amp;O 380</th>
<th>Assignment #2</th>
<th>Due: February 26, 1986</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1. $P$ is an arbitrary point on the circumcircle of equilateral triangle $ABC$. Prove that the smaller two of the lengths among $AP$, $BP$ and $CP$ add up to the biggest of them.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#2. What are the last 2 digits in the decimal representation of $21^{19^{18^{17}}}$ (i.e. $21^{19^{18^{17}}}$).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#3. Prove that the first 1000 digits after the decimal point in the decimal expansion of $(6 + \sqrt{35})^{1986}$ are all 9's.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#4. A circle of radius $\frac{1}{2}$ is tossed at random onto a coordinate plane. What is the probability that it covers a lattice point?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#5. A positive integer, of fewer than 25 digits, begins with the digits 15. The effect of multiplying this integer by 5 is merely to re-locate these first two digits to the end: $5(15abc\ldots k) = abc\ldots k15$. What is the integer?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#6. $A$ and $B$ take turns striking out a single number from a string of $n$ consecutive positive integers, $A$ going first. In order to eliminate special cases, suppose $n \geq 12$. The game ends when there are just two numbers left in the string, $A$ wins if the two numbers are relatively prime and $B$ wins if they are not. Devise (i) a winning strategy for $A$ in the case of $n$ odd, and (ii) a winning strategy for $B$ in the case when $n$ is even.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We will look at problem #2. These types of problems show up all the time in mathematics contests and introductory number theory courses. We have several paths of attack, each with its own merits.

First off, we can actually evaluate a few powers of 21 to see what we get

\[
21^0 = 1 \\
21^1 = 21 \\
21^2 = 441 \\
21^3 = 9261 \\
21^4 = 194 481 \\
21^5 = 4 084 101 \\
21^6 = 85 766 121 \\
21^7 = 1 801 088 541
\]

We are only interested in the last two digits and they seem to fall into a pattern 01, 21, 41, 61, 81, 01, 21, ... Does this pattern continue? If a number, \(N\), last two digits 01, 21, 41, 61 or 81, we can write it in the form \(N = 100m + 20n + 1\), where \(m\) and \(n\) are nonnegative integers and we can assume, without loss of generality, that \(0 \leq n \leq 4\). Then, if we multiply by 21 we get

\[
21N = 21(100m + 20n + 1) \\
= 2100m + 420n + 21 \\
= 2100m + 400n + 20n + 20 + 1 \\
= 100(21m + 4n) + 20(n + 1) + 1
\]

If \(n = 4\), then \(20(n + 1) = 100\) so \(21N = 100(21m + 4n + 1) + 1\), so the last digits of \(21^n\) follow the cycle 21 \(\rightarrow\) 41 \(\rightarrow\) 61 \(\rightarrow\) 81 \(\rightarrow\) 01 \(\rightarrow\) 21 \(\rightarrow\) ... as \(n\) goes through the positive integers.

Next, we have to find out where in the cycle we will be when we evaluate the expression. We can build up an argument, but there is a tool that will make the process much easier: modular arithmetic. We will say \(a \equiv b \pmod{n}\), read a is congruent to b modulo \(n\), if \(n \mid (a - b)\) (that is \(n\) divides evenly into \(a - b\)). This happens if \(a\) and \(b\) have the same remainder when divided by \(n\) (called the modulus). As a result, all integers are grouped into \(n\) groups, called equivalence classes. For example if we look at the integers modulo 6, we can write them as

<table>
<thead>
<tr>
<th></th>
<th>-11</th>
<th>-10</th>
<th>-9</th>
<th>-8</th>
<th>-7</th>
</tr>
</thead>
<tbody>
<tr>
<td>-6</td>
<td>-5</td>
<td>-4</td>
<td>-3</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>...</td>
</tr>
</tbody>
</table>

Then each column represents an equivalence class and all the numbers in that equivalence class are equivalent. Thus \(-10 \equiv 8 \pmod{6}\) since \(-10\) and 8 are in the same column and \(6 \mid (-10 - 8)\).

The equivalence relationship, congruence modulo \(n\), has several important properties. If \(a \equiv c \pmod{n}\) and \(b \equiv d \pmod{n}\) then:

1. \(a + b \equiv c + d \pmod{n}\),
2. \(ab \equiv cd \pmod{n}\),
3. \(a^m \equiv c^m \pmod{n}\) for any non-negative integer \(m\).

_Crux Mathematicorum_, Vol. 43(10), December 2017
This becomes useful because we can reduce numbers modulo $n$ and do the arithmetic with smaller numbers. In our case, we know that the last two digits of our expression will be 01, 21, 41, 61 or 81 corresponding to the exponent of 21 being congruent to 0, 1, 2, 3 or 4 modulo 5. Since 19 leaves a remainder of 4 when divided by 5, and 4 and $-1$ are “in the same column” (i.e. being 4 above a multiple of 5 is the same as being 1 below a [different] multiple of 5), we can write

$$19^{18^{17}} \equiv 4^{18^{17}} \equiv (-1)^{18^{17}} \equiv 1 \pmod{5}$$

since $18^{17}$ is clearly even. This means that $21^{19^{18^{17}}}$ has the same last two digits as $21^1 = 21$, so the last two digits are 21.

Now that we have modular arithmetic, we could have actually solved the problem another way. If we utilize the binomial theorem and the properties of equivalence modulo $n$ we would get

$$21^{19^{18^{17}}} = (20 + 1)^{19^{18^{17}}}$$

$$= \sum_{i=0}^{19^{18^{17}}} \binom{19^{18^{17}}}{i} 20^i$$

$$= \sum_{i=0}^{19^{18^{17}}} \binom{19^{18^{17}}}{i} 2^i \cdot 10^i$$

$$= \sum_{i=2}^{19^{18^{17}}} \binom{19^{18^{17}}}{i} 2^i \cdot 10^i + \binom{19^{18^{17}}}{1} 20 + \binom{19^{18^{17}}}{0}$$

$$\equiv \left(19^{18^{17}}\right) 20 + \left(19^{18^{17}}\right) 1 \pmod{100}$$

$$\equiv 20 \cdot 19^{18^{17}} + 1 \pmod{100}$$

Since $20 \times 5 \equiv 0 \pmod{100}$, we use that $19^{18^{17}} \equiv 1 \pmod{5}$ to get our result.

Modular arithmetic comes in handy many places. Search through some old math contests to find similar problems that ask for the last few digits of some expression that would be next to impossible to evaluate by hand. It is also the basis for a number of divisibility tests. For example, since $10 \equiv 1 \pmod{3}$, the well known test for divisibility by 3 pops out. Since we can write the $n$ digit number as $a_{n-1}a_{n-2} \cdots a_2a_1a_0 = \sum_{i=0}^{n-1} a_i10^i$, we get

$$\sum_{i=0}^{n-1} a_i1^i \pmod{3} \equiv a_{n-1} + a_{n-2} + \cdots + a_2 + a_1 + a_0 \pmod{3}.$$