THE CHINESE REMAINDER THEOREM

I want to turn now to a quite different problem. It concerns a result which has been known for centuries... Archimedes certainly knew it. It was also known somewhat later to the Chinese. For that reason it is called the Chinese Remainder Theorem.

**Theorem 43 (Chinese Remainder Theorem Mark 1)** There is a unique number $x$ modulo $m_1m_2\ldots m_n$ such that

\[
\begin{align*}
    x &\equiv a_1 \pmod{m_1} \\
    x &\equiv a_2 \pmod{m_2} \\
    x &\equiv a_3 \pmod{m_3} \\
    \vdots \\
    x &\equiv a_n \pmod{m_n},
\end{align*}
\]

for any integers $a_1, a_2, \ldots, a_n$, and for any integers $m_1, m_2, \ldots, m_n$ such that $(m_i, m_j) = 1$, for $i \neq j$.

Rather than prove this here, I just want to illustrate it with an example. We will solve the entirely representative system of congruences

\[
\begin{align*}
    x &\equiv 5 \pmod{11} \\
    x &\equiv -4 \pmod{7} \\
    x &\equiv 8 \pmod{9}
\end{align*}
\]

I call the first method of proof, the primary school method, because it uses nothing except the most elementary counting argument. We proceed as follows;

First write down all integers which solve the first congruence. They are

\[
\{ \ldots, 5, 16, 27, 38, 49, 60, 71, 82, 93, 104, 115, 126, 137 \ldots \}.
\]

Now I will write underneath each of these their remainder on division by the next modulus, namely 7. We get

<table>
<thead>
<tr>
<th>5</th>
<th>16</th>
<th>27</th>
<th>38</th>
<th>49</th>
<th>60</th>
<th>71</th>
<th>82</th>
<th>93</th>
<th>104</th>
<th>115</th>
<th>126</th>
<th>137</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

We can see that every possible remainder modulo 7 occurs on the second line of this array. We can also just read of the integers which solve the first two congruences, namely,

\[
\{ \ldots, 38, 115, 192, 269, 346, 423, 500, 577, 654, 731, 808, 885, \ldots \}.
\]
Notice that these integers all differ by $77 = 11 \cdot 7$ and so there is a unique integer modulo $11$, namely $38$ such that

\[
x \equiv 5 \pmod{11} \quad \text{and} \quad x \equiv -4 \pmod{7}.
\]

We can now proceed to the final congruence. Write underneath each of the solutions of the first two congruences the remainders on division by the last modulus 9.

\[
\begin{array}{cccccccccccc}
38 & 115 & 192 & 269 & 346 & 423 & 500 & 577 & 654 & 731 & 808 & 885 & 962 \\
2 & 7 & 3 & 8 & 4 & 0 & 5 & 1 & 6 & 2 & 7 & 3 & 8 \\
\end{array}
\]

We can now read off the complete solution of our system of congruences, namely,

\[
\ldots, 269, 962, 1655, 2348, 2987, \ldots
\]

Our second proof of the example, which I call the secondary school method, is slightly more sophisticated than this method, but only in the language we use to give it. Otherwise it is exactly the primary school method.

A complete solution of the first congruence consists of all integers $x = 5 + 11k$, for some integer $k$. To solve the second congruence, we need to solve

\[
5 + 11k \equiv -4 \pmod{7}
\]

and this needs $11k \equiv -9 \equiv 5 \pmod{7}$.

Now the inverse of $11 = 4$ modulo $7$ is $2$ and so dividing by 11, that is, multiplying by $2$ modulo $11$, we have

\[
k \equiv 10 \equiv 3 \pmod{7}
\]

and so $k = 3 + 7\ell$, for some integer $\ell$.

Hence

\[
x = 5 + 11k = 5 + 11(3 + 7\ell) = 38 + 11.7\ell.
\]

Notice that $38$ does in fact solve the first two congruences! It is also exactly what we got in the first approach.

Now we need to have our solution $x \equiv 8 \pmod{9}$. Thus we need $38 + 11.7\ell \equiv 8 \pmod{9}$ and so $11.7\ell \equiv 6 \pmod{9}$. The inverse of $11.7 \equiv 5 \pmod{9}$ is $2$. Dividing $5\ell \equiv 6 \pmod{9}$ by $5$, that is, multiplying by $2$ modulo $9$, we have $2.5\ell = 10\ell \equiv 12 \pmod{9}$ we have $\ell \equiv 3 \pmod{9}$.

Hence

\[
x = 38 + 11.7\ell = 38 + 11.7(3 + 9m) = 269 + 11.7.9m.
\]

Thus we have solved the system of congruences and the solution is unique (269) modulo $11.7.9$.

This is the Chinese Remainder Theorem Mark 1.

Remark: I won’t write a formal proof of the CRT here because we will give a much better version of it with a much easier proof in a little while. For now I want you to believe that it is true because you can do it with any particular example. Please try a couple.

As a side here to help you with units in different rings, I want to give you a result which will make the work easier. It holds in any integral domain which has a Euclidean Algorithm and so holds in $\mathbb{Z}$, $\mathbb{Z}[i]$ and $\mathbb{Z}_p[x]$ and many other rings.
**Theorem 44** Let $R$ be any integral domain which has a Euclidean Algorithm (and so, of course, a Division Algorithm). Then $R_a$ (R modulo $a$) is a field if and only if $a$ is a prime in $R$.

**Proof.**

Suppose $a \neq 0 \in R$ is not prime in $R$ but that $R_a$ is a field. We’ll derive a contradiction. Since $a$ is not prime, $a = xy$ where neither $x$ nor $y$ is a unit. If $a|x \in R$ then $x = au$ and $a = auy$ giving $uy = 1$ in the integral domain $R$ and so $y$ is a unit in $R$. This is not the case. Similarly $a$ does not divide $y$ in $R$. Hence $x, y \neq 0 \in R$. But $xy = a = 0 \in R_a$. But then $x$ and $y$ are zero divisors in $R_a$ and $R_a$ cannot be a field.

Conversely, suppose that $a$ is a prime in $R$ and suppose that $x \in R$ is any element which is not $\equiv 0 \pmod{a}$. The gcd $d = (a, x) = au + xv$ divides $a$ and so $a = dy$, for some $y$. Since $a$ is a prime either $y$ is a unit or $d$ is. If $y$ is a unit, then $d = ay^{-1} \equiv 0 \pmod{a}$, Since $d|x$ $x \equiv 0 \pmod{a}$, a contradiction. Hence $d$ is a unit in $R$. But then $1 = aud^{-1} + xvd^{-1}$ and $xvd^{-1} = 1 \in R_a$.

Hence $x$ is a unit in $R_a$ for any $x \neq 0 \in R_a$ and so $R_a$ is a field.

This completes the proof.

So for example to see if any particular element of $F = \mathbb{Z}_7[x]_{x^3+2x^2+x+4}$ is a unit (see for example Tutorial 8), it is better to see if every element has an inverse, that is to see if $F$ is a field. To do this, we need only check to see if $x^3 + 2x^2 + x + 4$ is prime in $\mathbb{Z}_7[x]$. As a cubic, if it has any non-trivial factors in $\mathbb{Z}_7[x]$ it has a linear factor and so a root in $\mathbb{Z}_7$. So we need only try the elements of $\mathbb{Z}_7$ and look for roots of $f(x) = x^3 + 2x^2 + x + 4 = 0 \in \mathbb{Z}_7$.

\[
\begin{align*}
  f(0) & = 4 \\
  f(1) & = 1 \\
  f(2) & = 1 \\
  f(3) & = 3 \\
  f(4) & = 6 \\
  f(5) & = 2 \\
  f(6) & = 4,
\end{align*}
\]

and so $f(x) = 0$ has no roots in $\mathbb{Z}_7$ and so $f(x)$ is a prime in $\mathbb{Z}_7[x]$ and and $\mathbb{F}$ is a field. Therefore any non-zero element in $\mathbb{F}$ has an inverse in $\mathbb{F}$ AND OF COURSE IF YOU WANT TO FIND THE INVERSE OF ANY ONE, YOU USE THE EUCLIDEAN ALGORITHM (as we did in Tutorial 8)! It works with the speed of light.

By the way, we know from Theorem 13 that $2 + 3i$ is a prime in $\mathbb{Z}[i]$ because $N(2 + 3i) = 13$ is prime in $\mathbb{Z}$. Hence $\mathbb{Z}[i]_{2+3i}$ is a field without any more calculation. Again we can find the inverses of any element of it using Euclid’s Algorithm, as we did at the start of the lecture, though of course the calculations are not at this stage very easy. That situation will improve.

Now for something completely different. I am continuing with the Chinese Raminder Theorem but it doesn’t exactly look like it for a while.

**NEW RINGS FROM OLD RINGS**
I want us here to learn how to produce new rings from old. Suppose that we have two rings \( R \) and \( S \). I want to produce a new ring called \( R \oplus S \). It consists of elements \((r, s)\) which are ordered pairs, where \( r \in R \) and \( s \in S \). To make \( R \oplus S \) into a ring we need to define addition and multiplication.

\[
\text{Addition: } (r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)
\]

\[
\text{Multiplication: } (r - 1, s_1)(r_2, s_2) = (r - 1r_2, s_1s_2).
\]

Thus calculation in the ring \( R \oplus S \) is just simultaneous calculation in the two rings \( R \) and \( S \), side by side. It is easy to check that \( R \oplus S \) satisfies the axioms A, M and D and so is a commutative ring if \( R \) and \( S \) are. Note that the zero element and the multiplicative identity of \( R \oplus S \) are \((0_R, 0_S)\) and \((1_R, 1_S)\), respectively.

The first thing to notice about \( R \oplus S \) is that it contains two subrings which look exactly like \( R \) and \( S \), namely

\[
R' = \{(r, 0_S) : r \in R\}
\]

\[
S' = \{0_R, s) : s \in S\}.
\]

In fact \( R \oplus S \) is built out of \( R' \) and \( S' \) in such a way that every element of \( R \oplus S \) is a sum of an element of \( R' \) and \( S' \). We call \( R \oplus S \) the direct sum of \( R \) and \( S \).

The first question which must arise is to decide whether \( R \oplus S \) is a genuinely new ring or not. For example, it is a serious question to ask whether \( \mathbb{Z} \oplus \mathbb{Z} \) is different from \( \mathbb{Z} \)? Is it possible that it might be the same as \( \mathbb{Z} \) in disguise? Don’t answer that there are ‘more’ elements in \( \mathbb{Z} \oplus \mathbb{Z} \). That’s not true. There is a \((1, 1)\) correspondence between these two sets. We need to look at this more closely.

**Definition** Two rings \( R \) and \( S \) are isomorphic if there is a dictionary correspondence (better a \((1, 1)\) correspondence) between the two rings which carries the multiplication and addition tables of one ring to the other. We can state that more formally as follows:

**Definition** An isomorphism \( \varphi : R \to S \) from the ring \( R \) to the ring \( S \) is a one-to-one correspondence such that

\[
\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)
\]

\[
\varphi(r_1r_2) = \varphi(r_1)\varphi(r_2),
\]

for all \( r_1, r_2 \in R \).

If \( R \) is isomorphic to \( S \) we write \( R \cong S \).

Note that the ring \( \mathbb{Z}[i] \) is obviously isomorphic to the ring \( \mathbb{Z}j = \{a + bj : a, b \in \mathbb{Z}, j^2 = -1\} \), since a name change \( \varphi(a + ib) = \varphi(a + jb) \) obviously remembers addition and multiplication.

Similarly \( R \cong R' = \{(r, 0_S) : r \in \mathbb{R}\} \), with isomorphism \( \varphi : R \to R' \varphi(r) = (r, 0_S) \).