Number Theory Reporting, Tutorial 3

Sean Diffley, Eric Hattaway, Conn McCarthy, Nathan O Duill, Michael Ferreira.

February 6, 2014

Question 1

Given $\tau : \mathbb{Z}/(ab)\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ defined as $\tau(n + ab\mathbb{Z}) = (n + a\mathbb{Z}, n + b\mathbb{Z})$ we need to prove that it is a ring homomorphism, that is, prove that the function τ preserves the operation of addition and multiplication.

$$\tau(x + y) = \tau(x) + \tau(y)$$
$$\tau(xy) = \tau(x)\tau(y)$$

If we write $x = (n_1 + (ab)\mathbb{Z})$ and $y = (n_2 + (ab)\mathbb{Z})$ then:

$$\tau((n_1 + (ab)\mathbb{Z}) + (n_2 + (ab)\mathbb{Z})) \to \tau((n_1 + n_2) + (ab)\mathbb{Z}) \to ((n_1 + n_2) + a\mathbb{Z}, (n_1 + n_2) + b\mathbb{Z}) \to$$
$$(n_1 + a\mathbb{Z}, n_1 + b\mathbb{Z}) + (n_2 + a\mathbb{Z}, n_2 + b\mathbb{Z})$$

where in the last step we are using the definition of addition of direct product of rings:

$$(r + r', s + s') = (r, s) + (r', s').$$

For multiplication we have:

$$\tau((n_1 + (ab)\mathbb{Z})(n_2 + (ab)\mathbb{Z})) \to \tau(n_1 n_2 + (ab)\mathbb{Z}) \to (n_1 n_2 + a\mathbb{Z}, n_1 n_2 + b\mathbb{Z}) \to$$
$$(n_1 + a\mathbb{Z}, n_1 + b\mathbb{Z})(n_2 + a\mathbb{Z}, n_2 + b\mathbb{Z})$$

where in the last step again we are using the definition of multiplication for direct product of rings:

$$(rr', ss') \to (r, s)(r', s').$$

It is clear that the identity maps to the identity because we can just substitute the identity for n in the above. So we have shown that τ preserves the operations of the ring and is hence a homomorphism.
Let us note that the kernel of this map is trivial, that is consists of zero only. For if

$$(n + a\mathbb{Z}, n + b\mathbb{Z}) = \tau(n + ab\mathbb{Z}) = (0, 0) = (a\mathbb{Z}, b\mathbb{Z}),$$

then n is divisible by a and by b, hence is divisible by ab since a and b are coprime, so $n + ab\mathbb{Z} = ab\mathbb{Z}$ which is 0 in $\mathbb{Z}/(ab)\mathbb{Z}$.
Finally, we use the First Isomorphism Theorem for rings which states that the image of a ring homomorphism $\phi\colon R \to S$ is isomorphic to the quotient ring $R/\ker(\phi)$. For finite rings, it implies that an injective homomorphism of two rings with the same number of elements is an isomophism. Since the rings $\mathbb{Z}/(ab)\mathbb{Z}$ and $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ both consist of ab elements, and τ is injective (since it has trivial kernel), we conclude that τ is an isomophism.

Question 2

$$\gcd(a, b) = 1$$

So

$$\begin{aligned}
&\Rightarrow ax + by = 1 \text{ for certain } x, y \\
&\Rightarrow ax = -by + 1 = r \\
&\Rightarrow r = 0 \mod a; r = 1 \mod b
\end{aligned}$$

Similarly,

$$\begin{aligned}
&\Rightarrow ax + by = 1 \text{ for certain } x, y \\
&\Rightarrow by = -ax + 1 = r \\
&\Rightarrow r = 1 \mod a \; ; r = 0 \mod b
\end{aligned}$$

For general m, n

$$\begin{aligned}
&ax + by = 1 \\
&\Rightarrow (n - m)(ax + by) = 1(n - m) \\
&\Rightarrow a(n - m)x + b(n - m)y = n - m \\
&\Rightarrow (n - m)x = x' \; ; (n - m)y = y' \\
&\Rightarrow ax' + by' = n - m \\
&\Rightarrow ax' + m = -by' + n = r \\
&\Rightarrow r = m \mod a \; ; r = n \mod b
\end{aligned}$$

Uniqueness trivially follows from the previous question.

Question 3

We need to solve the following system of equations:
$x \equiv 11(mod 23)$
$x \equiv 12(mod 25)$
$x \equiv 13(mod 27)$
Let $m_1 = 23$ $m_2 = 25$ $m_3 = 27$
and note that $\gcd(m_i, m_j) = 1, i \neq j$
which means that m_1, m_2, m_3 are pairwise coprime, and thus, by the Chinese Remainder Theorem, there exists a unique to the solution to the system of equations mod M, where $M = m_1.m_2.m_3$
Using modular arithmetic we can substitute x into each congruence to find the general solution.
Eq (1) can be rewritten as follows: $x = 11 + 23n_1$ where n_1 is an integer.

We substitute this into eq (2):
$11 + 23n_1 \equiv 12(mod 25)$ and solve for n_1:
$23n_1 \equiv 1(mod 25)$
$-2n_1 \equiv 1(mod 25)$
$13. - 2n_1 \equiv 13.1(mod 25)$
$-n_1 \equiv 13(mod 25)$
$n_1 \equiv -13(mod 25) \equiv 12(mod 25)$
or equivalently
$n_1 = 12 + 25n_2$
where n_2 is an integer. Now eq (1) can be rewritten as:
$x = 11 + 23(12 + 25n_2) = 287 + 575n_2$
We now substitute this representation of x into eq (3): $287 + 575n_2 \equiv 13(mod 27)$
$575n_2 \equiv -274(mod 27)$
$8n_2 \equiv 23(mod 27)$
$17.8n_2 \equiv 17.23(mod 27)$
$136n_2 \equiv 391(mod 27)$
$n_2 \equiv 13(mod 27)$
or equivalently,
$n_2 = 13 + 27n_3$
where n_3 is an integer. We substitute this into eq (1) again, which gives:
$x = 11 + 23(12 + 25[13 + 27n_3])$
$x = 11 + 23.12 + 23.25.13 + 23.25.27n_3$
$x = 7762 + 23.25.27n_3$
or equivalently, $x = 7762(mod M)$
where $M = m_1.m_2.m_3$, as required.
Question 4

$$\begin{aligned} x &\equiv a \mod 100 \\ x &\equiv b \mod 35 \end{aligned}$$

So

$$\begin{aligned} &\Rightarrow x = 100m + a = 35n + b \\ &\Rightarrow 100m - 35n = b - a \\ &\Rightarrow 5(20m - 7n) = b - a \end{aligned}$$

And

$$\begin{aligned} &gcd(100, 35) = 5 \\ &\Rightarrow 100r + 35q = 5 \text{ for some r, s} \\ &\Rightarrow 20r + 7q = 1 \\ &\Rightarrow s(20r + 7q) = s(1) \\ &\Rightarrow 20sr + 7sq = s \end{aligned}$$

Let

$$sr = r'; sq = q'$$

Then

$$\begin{aligned}
&20r' + 7q' = s, \text{ for any s} \\
&\Rightarrow 5s = b - a \\
&\Rightarrow b = a \mod 5
\end{aligned}$$

Which is equivalent to

$$a = b \mod 5$$

So, for all

$$a = b \mod 5,$$

The system of congruences

$$\begin{aligned}
x = a \mod 100 \\
x = b \mod 35
\end{aligned}$$

will have integer solutions.

Question 5

Suppose there are only finitely many such primes. Then $\exists$ some prime p s.t
$2p + 1, 2(2p + 1) + 1 = 4p + 3, ...$ and in general $2^n p + 2^n - 1$ is prime for all positive integers n.
To see that this formula holds in general, note that

$2(2^n p + 2^n - 1) + 1 = 2^{n+1} p + 2^{n+1} - 1$

In particular, letting $n = p - 1$, we get that $2^{p-1} p + (2^{p-1} - 1)$ is prime. But by Fermat's Little Theorem,
$2^{p-1} \equiv 1$ (mod p)
$2^{p-1} - 1 \equiv 0$ (mod p)
That is, $2^{p-1} - 1$ is an integer multiple of p. Thus $2^{p-1} p + (2^{p-1} - 1)$ is an integer multiple of p, contradicting the assumption that it is prime. Thus there are infinitely many such primes, as required.

Question 6

Let p be a prime divisor of $4n^2 + 1$
$4n^2 + 1 \equiv 0$ mod p
$(2n)^2 + 1 \equiv 0$ mod p
$\implies p \equiv 1$ mod 4 (given)
$\implies p = 4k + 1$, some integer k

As required. To prove there are infinitely many primes of this form, suppose there are only finitely man such primes, say $p_1, \cdots, p_n$

Consider $(2p_1p_2p_n)^2 + 1 = 4(p_1)^2...(p_n)^2 + 1$
This is not divisible by 2, or any of $p_1, ..., p_n$. Either it is prime, and thus is another prime of the form 4k+1, or it is divisible by a prime, which by above must be of the form 4k+1. In each case, we get an additional prime of the form 4k+1. Inductively there are infinite such primes.