Lemma 10 Let p and q be prime numbers with $p \neq q$ and let $n = p \cdot q$. Let $e \in \mathbb{N}$ be a natural number satisfying $\gcd(e, (p-1)\cdot(q-1)) = 1$. Then there exists $d \in \{1, \ldots, (p-1)\cdot(q-1)\}$ such that x^d is the inverse function of x^e on $\mathbb{Z}_n$. That means,

$$(x^e)^d = (x^d)^e = x \quad \text{for every } x \in \mathbb{Z}_n$$

Proof: We use the isomorphism of unitary rings

$$f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_q \qquad f([z]_n) = ([z]_p, [z]_q)$$

as in the proof of Theorem 9. We want to verify that $x^{ed} = x$ for every $x \in \mathbb{Z}_n$.

But since $\mathbb{Z}_n$ and $\mathbb{Z}_p \times \mathbb{Z}_q$ are isomorphic, it suffices to verify the same identity over $\mathbb{Z}_p \times \mathbb{Z}_q$ instead of $\mathbb{Z}_n$. Let's make a bit more formal.

It suffices to check that $f(x^{ed}) = f(x)$ for every $x \in \mathbb{Z}_{pq}$, because f is injective.

But since f is a homomorphism, the equality $f(x^{ed}) = f(x)$ is equivalent to $f(x)^{ed} = f(x)$.

Let $f(x) = (x_1, x_2)$, where $x_1 \in \mathbb{Z}_p$ and $x_2 \in \mathbb{Z}_q$.

Then $f(x)^{ed} = f(x)$ gets rewritten as

$$\begin{cases} x_1^{ed} = x_1 \\ x_2^{ed} = x_2 \end{cases}$$

Now, let us show that some $d \in \{1, \dots, (p-1)(q-1)\}$ satisfies these two identities.

By Theorem 6, $[e]_{(p-1)\cdot(q-1)}$ is invertible in $\mathbb{Z}_{(p-1)\cdot(q-1)}$. Hence, there exists $d \in \{1, \ldots, (p-1)\cdot(q-1)\}$ such that

$$[e]_{(p-1)(q-1)} \cdot [d]_{(p-1)\cdot(q-1)} = [1]_{(p-1)\cdot(q-1)}.$$

(Such d can be computed using the EEA.)

That means, $e \cdot d = 1 + k \cdot (p-1)\cdot(q-1)$ for some non-negative integer k. Hence,

$$x_1^{ed} = x_1^{1+k(p-1)(q-1)} = x_1 \cdot \left(x_1^{p-1}\right)^{k(q-1)} \overset{(*)}{=} x_1$$

$(x_1 \in \mathbb{Z}_p)$

$(*)$ Fermat's Little Theorem (Theorem 7)

Just the same thing for $x_2 \in \mathbb{Z}_q$:

$$x_2^{ed} = x_2^{1+k(p-1)(q-1)} = x_2 \cdot \left(x_2^{q-1}\right)^{k(p-1)} = x_2. \quad \square$$

1.5 RSA Cryptosystem

See Presentation

For decryption we apply x^d for $x \in \mathbb{Z}_n$.
We use fast exponentiation to make it fast, despite the fact d is large. But a large n is also a problem in terms of efficiency of computations.
We can go from $\mathbb{Z}_n$ to $\mathbb{Z}_p \times \mathbb{Z}_q$, but then we need to go back. How to do this computationally?
We can use

Proposition 11 For integers $n, n_1, n_2 \geq 2$, with $n = n_1 n_2$ and $\gcd(n_1, n_2) = 1$ the inverse of the unitary ring isomorphism $f: \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$
$f([z]_n) = ([z]_{n_1}, [z]_{n_2})$ can be given as
$f^{-1}([z_1]_{n_1}, [z_2]_{n_2}) = [a_1 z_1 + a_2 z_2]_n$ where

$a_1, a_2 \in \mathbb{Z}$ are appropriately chosen integer values.

Proof: The EEA gives $s_1, s_2 \in \mathbb{Z}$ with $\underbrace{s_1 n_1}_{=a_2} + \underbrace{s_2 n_2}_{=a_1} = 1$

One has $a_1 z_1 + a_2 z_2 \equiv a_1 z_1 \equiv (1 - s_1 n_1) z_1 \equiv z_1 \pmod{n_1}$
and $a_1 z_1 + a_2 z_2 \equiv a_2 z_2 \equiv (1 - s_2 n_2) z_2 \equiv z_2 \pmod{n_2}$,
which shows that the formula for the inverse is correct. □

Example

$\mathbb{Z}_5 \times \mathbb{Z}_7 \to \mathbb{Z}_{35}$

$n_1 = 5$
$n_2 = 7$ EEA ⇝

$$\begin{cases} n_1 = 5 \\ n_2 = 7 \end{cases}$$

$$\begin{cases} n_1 = 5 \\ -n_1 + n_2 = 2 \end{cases}$$

$$\begin{cases} 3n_1 - 2n_2 = 1 \\ -n_1 + n_2 = 2 \end{cases}$$

$$\Downarrow$$

$3 \cdot 5 - 2 \cdot 7 = 1$

$15 - 14 = 1$, where

$15 \equiv 0 \pmod 5$ $\quad -14 \equiv 1 \pmod 5$
$15 \equiv 1 \pmod 7$ $\quad -14 \equiv 0 \pmod 7$

$$f^{-1}([z_1]_5, [z_2]_7) = [-14 z_1 + 15 z_2]_{35}$$

Let's follow up on the example in the beginning of 1.4 and compute

$$f^{-1}([1]_5, [5]_7) = [-14 \cdot 1 + 15 \cdot 5]_{35}$$
$$= [61]_{35} = [26]_{35}$$