Introduction to Number Theory
4. exercise set, solutions

1. Write $p = ab$ with $1 < a, b < p$. If $a \neq b$, then both numbers appear in the product $(p-1)!$. Thus $(p-1)! + 1 \equiv 1 \not\equiv 0 \pmod p$. If $a = b$ and $p > 4$, we have $1 < a < 2a \leq p - 1$. Hence the numbers a and $2a$ appear in the product $(p-1)!$ so $a^2 = p$ divides it. The remaining case $p = 4$ is easy to handle. $\square$

2. Recall that $a \in \mathbb{Z}_p^*$ is a primitive root modulo p if and only if $\mathrm{ord}_p(a) = \varphi(p)$.

(i) It is enough to calculate the orders of $1, 2, ..., 10$ and check that which of them equal to $\varphi(p) = 10$. This is straightforward to do and one sees that the primitive roots mod 11 are $2, 6, 7$ and 8.

(ii) It is enough to calculate the orders of $1, 2, ..., 17$ and check that which of them equal to $\varphi(p) = 6$. This is straightforward to do and one sees that the primitive roots mod 18 are 5 and 11.

3. Note that $\mathrm{ord}_{73}(2)$ divides $\varphi(73) = 72$. Thus $\mathrm{ord}_{73}(2)$ is of the form $2^\alpha 3^\beta$ for $0 \leq \alpha \leq 3$, $0 \leq \beta \leq 2$. The smallest of these numbers s.t. $2^\ell \equiv 1 \pmod{73}$ is 9 so $\mathrm{ord}_{73}(2) = 9$. Similar reasoning gives $\mathrm{ord}_{73}(7) = 24$.

It follows that

$$14^{72} \equiv 7^{72} \cdot 2^{72} \equiv (7^{24})^3 \cdot (2^9)^8 \equiv 1 \cdot 1 \equiv 1 \pmod{73},$$

so 14 might be a primitive root mod 73. This is easy to confirm.

4. Note first that $1125 = 3^2 \cdot 5^3$. Let $f(x) = x^3 - 3x^2 + 27$ and note that $f'(x) = 3x^2 - 6x$. Consider first the congruence $f(x) \equiv 0 \pmod 3 \Leftrightarrow x^3 \equiv 0 \pmod 3 \Leftrightarrow x \equiv 0 \pmod 3$.

Consider then $f(x) \equiv 0 \pmod{3^2} \Rightarrow f(x) \equiv 0 \pmod 3 \Rightarrow x \equiv 0 \pmod 3$. Conversely, if $x \equiv 0 \pmod 3 \Rightarrow x = 3t \Rightarrow f(x) = f(3t) = 27t^3 - 27t^2 + 27 \equiv 0 \pmod{3^2}$. Hence $f(x) \equiv 0 \pmod{3^2}$ if and only if $x \equiv 0 \pmod 3$.

Consider next the congruence $f(x) \equiv 0 \pmod 5 \Leftrightarrow x^3 - 3x^2 + 2 \equiv 0 \pmod 5$. It is easy to check by hand that the only solution is $x \equiv 1 \pmod 5$. Consider then $f(x) \equiv 0 \pmod{5^2}$ $\Rightarrow f(x) \equiv 0 \pmod 5 \Rightarrow x \equiv 1 \pmod 5$. Conversely, suppose that $x \equiv 1 \pmod 5 \Rightarrow x = 5t+1$. Then by the Taylor expansion

$$f(x) = f(5t+1) \equiv f(1) + f'(1) \cdot 5t \equiv 0 - 15t \equiv 10t \equiv 0 \pmod{5^2} \Leftrightarrow t \equiv 0 \; (\mathrm{mod} 5).$$

Thus $x = 5t + 1 = 25t' + 1 \equiv 1 \pmod{5^2}$.

Finally consider $f(x) \equiv 0 \pmod{5^3} \Rightarrow f(x) \equiv 0 \pmod{5^2} \Rightarrow x = 25t' + 1$. Conversely, if $x = 25t' + 1$ then by the Taylor expansion

$$f(x) = f(25t'+1) \equiv f(1) + f'(1) \cdot 25t' \equiv 25 - 3 \cdot 25t' \equiv 0 \pmod{5^3} \Leftrightarrow 1 - 3t' \equiv 0 \pmod 5.$$

This holds only when $t' \equiv 2 \pmod 5$. Now $x = 25t' + 1 = 1 + 25(2 + 5t'') \equiv 51 \pmod{5^3}$. Hence $f(x) \equiv 0 \pmod{1125}$ if and only if $x \equiv 0 \pmod 3$ and $x \equiv 51 \pmod{5^3}$. This gives that $x \equiv 51, 426, 801 \pmod{1125}$.

5. Let p be an integer s.t. $(p, 10) = 1$. Define a sequence $a_1, a_2, a_3, ...$ in the following way. Set $a_1 = 1$ and

$$a_{k+1} = 10\left(a_k - p\left\lfloor \frac{a_k}{p} \right\rfloor\right).$$

Note that a_k's are non-negative integers. Thinking how the division algorithm works one sees that the element a_k uniquely determines the k^{th} digit of $1/p$. Namely, if $1/p = 0.b_2b_3b_4...$ then

$$b_k = \left\lfloor \frac{a_k}{p} \right\rfloor.$$

As a_k determines a_{k+1} and a_k determines b_k it suffices to show that $a_\ell = a_2$ for some $\ell > 2$ in order to show that the decimal expansion of $1/p$ is periodic.

The crucial observation is that $a_{k+1} = a_{\ell+1}$ if and only if $p | a_k - a_\ell$. Indeed, if $a_{k+1} = a_{\ell+1}$, then

$$a_k - p\left\lfloor \frac{a_k}{p} \right\rfloor = a_\ell - p\left\lfloor \frac{a_\ell}{p} \right\rfloor$$

i.e.

$$a_k - a_\ell = p\left(\left\lfloor \frac{a_k}{p} \right\rfloor - \left\lfloor \frac{a_\ell}{p} \right\rfloor\right)$$

which shows that $p | a_k - a_\ell$. The other direction is obvious.

Hence we only need to find $\ell \in \mathbb{Z}_+$ s.t. $a_\ell \equiv 1 \pmod{p}$ as $a_1 = 1$. From the definition of a_k it follows that $a_k \equiv 10^{k-1} \pmod{p}$ for every $k \geq 1$. As $(p, 10) = 1$ we have by Euler's theorem

$$a_{\varphi(p)+1} \equiv 10^{\varphi(p)} \equiv 1 \pmod{p}.$$

Therefore we can choose $\ell = \varphi(p) + 1$ which finally shows that the decimal expansion of $1/p$ is periodic. □

6. We prove the statement first for monomials $f(x) = x^n$, $n \geq 0$. If $k > n$, then $f^{(k)} = 0$ so $k! | f^{(k)}(y)$. If $0 < k \leq n$, then

$$f^{(k)}(x) = n(n-1)\cdots(n-k+1)x^{n-k} = \binom{n}{k} k! x^{n-k}$$

so $k! | f^{(k)}(y)$. Finally, if $k = 0$ then $k! = 1 | f(y)$.

The general case for $f(x) = a_\ell x^\ell + a_{\ell-1}x^{\ell-1} + \cdots + a_1 x + a_0$ follows by applying above to each summand separately. □

7. Recall that $\{\overline{1}, \overline{2}, ..., \overline{p-1}\}$ is a field as p is a prime. Thus every element has a multiplicative inverse in this field (this is seen, for example, by using Bezout's theorem). Note that only $\overline{1}$ and $\overline{p-1}$ are their own inverses. Furthermore two distinct elements cannot have same inverse. This is seen as follows. Suppose that x and y have the same inverse a. Then $ax \equiv 1 \pmod{p}$ and $ay \equiv 1 \pmod{p}$. Now $ax \equiv ay \pmod{p}$. As $(a, p) = 1$ it follows that $x \equiv y \pmod{p}$ which implies that x and y belong to the same residue class. Above observations mean that we can pair the elements of the set $\{\overline{2}, \overline{3}, ..., \overline{p-2}\}$ in the desired way. □

Now Wilson's theorem follows immediately. Pair each number and it's multiplicative inverse. Their product equals one (mod p) so $(p-1)! \equiv 1 \cdots 1 \cdot (p-1) \equiv -1 \pmod{p}$. □

8*. We know that $a^3 \equiv 1 \pmod{p}$. Thus $p | (a-1)(a^2 + a + 1)$. As $\text{ord}_p(a) = 3$ we have $a \not\equiv 1 \pmod{p}$. Thus $a^2 + a \equiv -1 \pmod{p}$. Note that

$$\begin{aligned}
(a+1)^6 &= a^6 + 6a^5 + 15a^4 + 20a^3 + 15a^2 + 6a + 1 \\
&\equiv a^6 + 6a^2 + 15a + 20 + 15a^2 + 6a + 1 \\
&\equiv 21(a^2 + a + 1) + 1 \\
&\equiv 1 \pmod{p}.
\end{aligned}$$

Hence $\text{ord}_p(a+1)|6$. If $\text{ord}_p(a+1) = 1$ then $a \equiv 0 \pmod{p}$ which is impossible. If $\text{ord}_p(a+1) = 2$ then $a^2 + 2a \equiv 0 \pmod{p}$ which is also impossible. If $\text{ord}_p(a+1) = 3$ then $1 \equiv (a+1)^3 = a^3 + 3(a^2 + a) + 1 \equiv -1 \pmod{p}$ which is a contradiction . Therefore $\text{ord}_p(a+1) = 6$. $\square$