Solutions #6

1. Let $a$ and $b$ be positive integers and let $a = qb + r$, where $0 \leq r < b$. Prove that

(a) $2^a - 1 \equiv 2^r - 1 \pmod{2^b - 1}$;
(b) $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a, b)} - 1$.

**Solution.** (a) Since $2^b - 1 \equiv 1 \pmod{2^b - 1}$, we have
\[
2^a - 1 = 2^{q(b + r)} - 1 = (2^b)^q(2^r - 1) \equiv 2^r - 1 \pmod{2^b - 1}.
\]

(b) Since $0 \leq 2^r - 1 < 2^b - 1$, part (a) shows that dividing $2^a - 1$ by $2^b - 1$ with a remainder, we get $2^a - 1 = Q(2^b - 1) + 2^r - 1$. Moreover, the fact that $2^r - 1 = 0$ if and only if $r = 0$, shows that the Euclid algorithm applies in parallel to the pairs $(a, b)$ and $(2^a - 1, 2^b - 1)$. More precisely, we have

\[
\begin{align*}
a &= q_1b + r_1 & 2^a - 1 &= Q_1(2^b - 1) + 2^{r_1} - 1 \\
b &= q_2r_1 + r_2 & 2^b - 1 &= Q_2(2^{r_1} - 1) + 2^{r_2} - 1 \\
r_1 &= q_3r_2 + r_3 & 2^{r_1} - 1 &= Q_3(2^{r_2} - 1) + 2^{r_3} - 1 \\
\vdots & \vdots & \vdots & \vdots \\
r_{n-2} &= q_nr_{n-1} + r_n & 2^{r_{n-2}} - 1 &= Q_n(2^{r_{n-1}} - 1) + 2^{r_n} - 1 \\
r_{n-1} &= q_{n+1}r_n & 2^{r_{n-1}} - 1 &= Q_{n+1}(2^{r_n} - 1).
\end{align*}
\]

This proves that, if \( \gcd(a, b) = r_n \), then \( \gcd(2^a - 1, 2^b - 1) = 2^{r_n} - 1 \). □

2. In this problem we want to find the number of solutions of the equation $x^2 = 1$ in $\mathbb{Z}_N$.

(a) Find the number of solutions of $x^2 = 1$ in $\mathbb{Z}_2$, $\mathbb{Z}_4$, and in $\mathbb{Z}_{2^k}$ for $k \geq 3$.
(b) Find the number of solutions of $x^2 = 1$ in $\mathbb{Z}_{p^k}$, where $p$ is an odd prime and $k \geq 1$.
(c) Find the number of solutions of $x^2 = 1$ in $\mathbb{Z}_N$, where $N = 2^k p_1^{k_1} p_2^{k_2} \ldots p_l^{k_l}$. Here $k \geq 0$, $k_1, k_2, \ldots, k_l \geq 1$ and $p_1, p_2, \ldots, p_l$ are distinct odd primes.

**Solution.** (a) In $\mathbb{Z}_2$ the equation $x^2 = 1$ has a unique solution $x = 1$ and in $\mathbb{Z}_4$ the equation $x^2 = 1$ has two solutions $x = 1$ and $x = 3$.

Let $k \geq 3$ and consider the equation $x^2 = 1$ in $\mathbb{Z}_{2^k}$. If $x = [a]_{2^k}$, where $a \in \mathbb{Z}$, the equation $x^2 = 1$ is equivalent to the condition that $2^k$ divides $a^2 - 1 = (a-1)(a+1)$. Since either both $a-1$ and $a+1$ are even or both are odd, they both need to be even. In that case \( \gcd(a - 1, a + 1) = 2 \) (Why?) and hence $2^k$ divides $a^2 - 1$ if and only if $2^{k-1}$ divides $a - 1$ or $2^{k-1}$ divides $a + 1$. Furthermore, $2^{k-1}$ divides $a - 1$ if and only if $a = 2^{k-1}q + 1$, i.e., if and only if $x = 1$ or $x = 2^{k-1} + 1$ in $\mathbb{Z}_{2^k}$. Analogously, $2^{k-1}$ divides $a + 1$ if and only if $a = 2^{k-1}q - 1$, i.e., if and only if $x = -1$ or $x = 2^{k-1} - 1$ in $\mathbb{Z}_{2^k}$. In short, $x^2 = 1$ has exactly 4 solutions in $\mathbb{Z}_{2^k}$ when $k \geq 3$. 

MATH210: page 1 of 4
(b) In the notations of (a), \( x^2 = 1 \) in \( \mathbb{Z}_{p^k} \) if and only if \( p^k \) divides \((a - 1)(a + 1)\). Since \( \gcd(a - 1, a + 1) = 1 \) or 2 (Why?), we conclude that \( p^k \) divides \((a - 1)(a + 1)\) if and only if \( x = \pm 1 \) in \( \mathbb{Z}_{p^k} \), i.e., \( x^2 = 1 \) has exactly 2 solutions in \( \mathbb{Z}_{p^k} \) when \( p \) is odd.

(c) Since the numbers \( 2^k, p_1^{k_1}, \ldots, p_l^{k_l} \) are pairwise co-prime \( x^2 = 1 \) in \( \mathbb{Z}_N \) is equivalent to the system of linear congruences for \( a \)

\[
\begin{align*}
(1) & \quad a^2 &\equiv 1 \pmod{2^k}, \quad a^2 &\equiv 1 \pmod{p_1^{k_1}}, & \ldots, & \quad a^2 &\equiv 1 \pmod{p_l^{k_l}}. \\
(2) & \quad a &\equiv \alpha_0 \pmod{2^k}, \quad a^2 &\equiv \alpha_1 \pmod{p_1^{k_1}}, & \ldots, & \quad a^2 &\equiv \alpha_l \pmod{p_l^{k_l}},
\end{align*}
\]

The first of these congruences is equivalent to \( a \) satisfying one of 1, 2, or 4 congruences of the type \( a \equiv \alpha \pmod{2^k} \) depending on whether \( k = 1, 2 \) or \( k \geq 3 \). (Here \( \alpha = 1 \) in \( \mathbb{Z}_2 \), \( \alpha = \pm 1 \) in \( \mathbb{Z}_4 \), and \( \alpha = \pm 1, 2^{k-1} \pm 1 \) in \( \mathbb{Z}_{2^k} \) for \( k \geq 3 \).

Each of the remaining congruences \( a^2 \equiv 1 \pmod{p_j^{k_j}} \), where \( 1 \leq j \leq l \), is equivalent to \( a \equiv \pm 1 \pmod{p_j^{k_j}} \). Hence \( a \) satisfying (1) is equivalent to \( a \) satisfying one of the systems

\[
(2) & \quad a &\equiv \alpha_0 \pmod{2^k}, \quad a^2 &\equiv \alpha_1 \pmod{p_1^{k_1}}, & \ldots, & \quad a^2 &\equiv \alpha_l \pmod{p_l^{k_l}},
\]

where \( \alpha_0 \) can take 1, 2, or 4 values, as described above, and each \( \alpha_j \) for \( 1 \leq j \leq l \) can take one of two values. The Chinese Remainder Theorem implies that each of the systems (2) is equivalent to a unique congruence \( a \equiv \beta \pmod{N} \) and hence to a unique solution \( [\beta]_N \) of \( x^2 = 1 \) in \( \mathbb{Z}_N \). Moreover, different systems (2) give different solutions of \( x^2 = 1 \) in \( \mathbb{Z}_N \) (Why?). Thus, \( x^2 = 1 \) has as many solutions in \( \mathbb{Z}_N \) as there are systems (2). Hence, the desired number of solutions is

\[
\begin{align*}
2^l & \quad \text{if } 0 \leq k \leq 1 \\
2^{l+1} & \quad \text{if } k = 2 \\
2^{l+2} & \quad \text{if } 3 \leq k. \\
\end{align*}
\]

3. Let \( \mathbb{F} \) be a field. Two variations of the ring of polynomial over \( \mathbb{F} \) are the formal power series \( \mathbb{F}[[X]] \) and the formal Laurent series \( \mathbb{F}((X)) \) defined as follows:

\[
\mathbb{F}[[X]] = \{ a_0 + a_1 X + a_2 X^2 + \ldots | a_i \in \mathbb{F} \}
\]

and

\[
\mathbb{F}((X)) = \{ a_{-k} X^{-k} + a_{-k+1} X^{-k+1} + a_{-k+2} X^{-k+2} + \ldots | k \in \mathbb{Z}, a_i \in \mathbb{F} \}.
\]

Show that both \( \mathbb{F}[[X]] \) and \( \mathbb{F}((X)) \) are integral domains. (Please, do not submit your work on this part!)

(a) Prove that

\[
(\mathbb{F}[[X]])^\times = \{ a_0 + a_1 X + a_2 X^2 + \ldots \in \mathbb{F}[[X]] | a_0 \neq 0 \}.
\]

(b) Find the inverses of \( 1 + X \) and \( 1 - X - X^2 \) in \( \mathbb{F}[[X]] \).

(c) Prove that \( \mathbb{F}((X)) \) is a field.
Solution. Verifying that \( \mathbb{F}[X] \) and \( \mathbb{F}(X) \) are commutative rings is analogous to verifying that \( \mathbb{F}[X] \) is a commutative ring. The fact that neither \( \mathbb{F}[X] \) nor \( \mathbb{F}(X) \) have zero divisors follows from the formula
\[
(a_k x^k + a_{k+1} x^{k+1} + \ldots) (b_l x^l + b_{l+1} x^{l+1} + \ldots) = a_k b_l x^{k+l} + (a_k b_{l+1} + a_{k+1} b_l) x^{k+l+1} + \ldots
\]
since the assumption \( a_k \neq 0 \) and \( b_l \neq 0 \) implies \( a_k b_l \neq 0 \). Informally, the lowest term of \( fg \) is the product of the lowest terms of \( f \) and \( g \) and, in over a filed, it cannot be zero.

(a) Assuming that \( fg = 1 \) with \( f, g \in \mathbb{F}[X] \), we conclude that \( a_0 b_0 = 1 \), i.e., \( a_0 \neq 0 \). This proves that
\[
(\mathbb{F}[X])^x \subset \{a_0 + a_1 X + a_2 X^2 + \ldots \in \mathbb{F}[X] | a_0 \neq 0 \}.
\]
Conversely, assume that \( f = a_0 + a_1 X + a_2 X^2 + \ldots \in \mathbb{F}[X] \) satisfies \( a_0 \neq 0 \). It is a unit if there is \( g = b_0 + b_1 X + b_2 X^2 + \ldots \in \mathbb{F}[X] \) such that \( fg = 1 \). Since
\[
fg = \sum_{n=0}^{\infty} \left( \sum_{j=0}^{k} a_j b_{k-j} \right) X^n,
\]
is equivalent to the system of equations for \( b_0, b_1, \ldots \)
\[
\begin{align*}
a_0 b_0 &= 1 \\
a_0 b_1 + a_1 b_0 &= 0 \\
& \vdots \\
a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0 &= 0 \\
a_0 b_{k+1} + a_1 b_k + \ldots + a_{k+1} b_0 &= 0 \\
& \vdots \\
\end{align*}
\]
Having solved the first \( k \) equations for \( b_0, b_1, \ldots, b_k \), the \( (k+1) \)-st equation is a linear equation for \( b_{k+1} \). Moreover, solving it depends only on whether \( a_0^{-1} \) exists. Hence, assuming that \( a_0 \neq 0 \) we can solve the system (3) and, hence, we can find \( g \) such that \( fg = 1 \). This completes the proof \( f \in \mathbb{F}[X])^x \), i.e., that
\[
\{a_0 + a_1 X + a_2 X^2 + \ldots \in \mathbb{F}[X] | a_0 \neq 0 \} \subset (\mathbb{F}[X])^x.
\]

(b) In this part we need to solve (3) for \( f = 1 + X \) and for \( f = 1 - X - X^2 \).

When \( f = 1 + X \), the system (3) becomes
\[
\begin{align*}
b_0 &= 1, & b_1 + b_0 &= 0, & b_2 + b_1 &= 0, & b_3 + b_2 &= 0, \ldots \\
\end{align*}
\]
with solution \( b_k = (-1)^k \). Hence the inverse of \( 1 + X \) is \( 1 - X + X^2 - X^3 + \ldots \).

When \( f = 1 - X - X^2 \), the system (3) becomes
\[
\begin{align*}
b_0 &= 1, & b_1 + b_0 &= 0, & b_2 - b_1 - b_0 &= 0, & b_3 + b_2 - b_1 &= 0, & b_4 - b_3 - b_2 &= 0, \ldots \\
\end{align*}
\]
The solution is the sequence \( b_0 = b_1 = 1, b_k = b_{k-1} + b_{k-2} \) for \( k \geq 3 \). But this is just the Fibonacci sequence with the index shifted by one, i.e., \( b_k = F_{k+1} \), see Problem 1 from Assignment 1. Thus the inverse of \( 1 - X - X^2 \) is
\[
F_1 + F_2X + F_3X^2 + F_4X^3 + \ldots
\]

(e) Let \( f \neq 0 \) be an element of \( \mathbb{F}((X)) \) with a leading term \( a_{-k}X^{-k} \), i.e., \( a_{-k} \neq 0 \). Then, by (a), \( X^k f \in (\mathbb{F}[[X]])^\times \). Let \( g \in (\mathbb{F}[[X]])^\times \) be the inverse of \( X^k f \), i.e., \( (X^k f)g = 1 \).
Then \( f(X^k g) = 1 \), i.e., \( X^k g \in \mathbb{F}((X)) \) is the inverse of \( f \). This proves that any nonzero element of \( \mathbb{F}((X)) \) has an inverse and thus \( \mathbb{F}((X)) \) is a field. \( \square \)