Cryptography I, homework sheet 5
Due: 21 October 2011, 10:45

1. Find the smallest positive integer x satisfying the following system of congruences, should such a solution exist.

$$\begin{aligned} x &\equiv 3 \bmod 4 \\ x &\equiv 6 \bmod 12 \end{aligned}$$

2. Find the smallest positive integer x satisfying the following system of congruences, should such a solution exist.

$$\begin{aligned} x &\equiv 4 \bmod 9 \\ x &\equiv 10 \bmod 12 \end{aligned}$$

3. Users A, B, C, D, and E are friends of S. They have public keys $(e_A, n_A) = (5, 62857), (e_B, n_B) = (5, 64541), (e_C, n_C) = (5, 69799), (e_D, n_D) = (5, 89179)$, and $(e_E, n_E) = (5, 82583)$. You know that S sends the same message to all of them and you observe the ciphertexts $c_A = 11529, c_B = 60248, c_C = 27504, c_D = 43997$, and $c_E = 44926$. What was the message?

4. Show how to retrieve the message m in RSA-OAEP from $m'||r'$.

5. The $n \times n$ matrices over $\mathbb{R}$ form a vectorspace over $\mathbb{R}$, where $\oplus$ is matrix addition and for $a \in \mathbb{R}$ and $A \in M_n(\mathbb{R})$ the operation $a \odot A$ is defined as multiplying every entry in A by a. (You do not need to show this.) What is the dimension of $M_n(\mathbb{R})$ as an $\mathbb{R}$ vectorspace?

The following is an excerpt from the algebra and number theory script, check there for more details on vector spaces and field.

Definition 1 (Field)
A set K is a field *with respect to two operations $\circ, \diamond$ denoted by $(K, \circ, \diamond)$ if*

1. *$(K, \circ)$ is an abelian group.*

2. *$(K^*, \diamond)$ is an abelian group, where $K^* = K \backslash \{e_\circ\}$ is all of K except for the neutral element with respect to $\circ$.*

3. *The distributive law holds in K:*

$$a \diamond (b \circ c) = a \diamond b \circ a \diamond c \text{ for all } a, b, c \in K.$$

Let L be a field and $K \subseteq L$. If K is a field itself it is a subfield *of L and L is an* extension field *of K.*

Definition 2 (Vector space)
A set V is a vector space *over a field $(K, \circ, \diamond)$ with respect to one operation $\oplus$ if*

1. *$(V, \oplus)$ is an abelian group.*

2. *$(K, \circ, \diamond)$ is a field. Let $e_\circ, e_\diamond$ be the neutral elements with respect to $\circ$ and $\diamond$.*

3. *There exists an operation* $\odot : K \times V \to V$ *such that for all* $a, b \in K$ *and for all* $\underline{v}, \underline{w} \in V$ *we have*

$$\begin{aligned} (a \circ b) \odot \underline{v} &= a \odot \underline{v} \oplus b \odot \underline{v} \\ a \odot (\underline{v} \oplus \underline{w}) &= a \odot \underline{v} \oplus a \odot \underline{w} \\ e_\diamond \odot \underline{v} &= \underline{v} \end{aligned}$$

Example Consider the field $(\mathbb{R}, +, \cdot)$ and define an operation on the 3-tuples $(x, y, z) \in \mathbb{R}^3$ by componentwise addition $(x_1, y_1, z_1) \oplus (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$ and for $a \in \mathbb{R}$ let $a \odot (x_1, y_1, z_1) = (ax_1, ay_1, az_1)$.
Since $\mathbb{R}$ is closed under addition and multiplication and since the distributive laws hold we have that $\mathbb{R}^3$ forms a vector space over $\mathbb{R}$ with these operations.
The same holds for $\mathbb{R}^n$ for any integer n. Usually we replace $\oplus$ by $+$ and omit $\odot$ in $\mathbb{R}^n$.

Example The complex numbers $\mathbb{C}$ form a vector space over the reals $(\mathbb{R}, +, \cdot)$ where the operations are defined as follows:
$\oplus$ is the standard addition of complex numbers, i.e. $(a + bi) \oplus (c + di) = (a + c) + (b + d)i$, and $\odot$ is the standard multiplication, i.e. $a \odot (b + ci) = (a \cdot b) + (a \cdot c)i$, in which the first argument is restricted to $\mathbb{R}$.
This fulfills the definition since we have already seen that $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are both fields. The last three conditions are automatically satisfied since $\mathbb{C}$ is a field.

The example of $\mathbb{C}$ being a vector space over $\mathbb{R}$ can be generalized to arbitrary extension fields.

Example Let $(K, \circ, \diamond)$ be a field and let $L \supseteq K$ be an extension field of K. Then L is a vector space over K, where $\oplus = \circ$ and $\odot = \diamond$.

Example Let K be a field and consider the polynomial ring $K[x]$ over K. We define $\oplus$ to be the coefficientwise addition, i.e. the usual addition in $K[x]$ and $\odot$ as the multiplication of each coefficient by a scalar from K, i.e. polynomial multiplication restricted to the case that one input polynomial is constant. Since $K[x]$ is a ring and K is a field, $K[x]$ is a vector space over K.

Example Let K be a field, $n \in \mathbb{N}$ and consider the subset P_n of $K[x]$ of polynomials of degree at most n, i.e. $P_n = \{f(x) \in K[x] | \deg(f) \leq n\}$. Since addition of polynomials and multiplication by constants do not increase the degree, P_n is closed under addition and multiplication by scalars from K and is thus a K-vector space.

Definition 3 (Linear combination, basis, dimension)
Let V *be a vector space over the field* K *and let* $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n \in V$.
A linear combination *of the vectors* $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n$ *is given by*

$$\sum_{i=1}^{n} \lambda_i \odot \underline{v}_i,$$

for some $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$, *where the summation sign stands for repeated application of* $\oplus$.
The elements $\underline{v}_1, \ldots, \underline{v}_n$ *are* linearly independent *if* $\sum_{i=1}^{n} \lambda_i \odot \underline{v}_i = e_\oplus$ *implies that for all* $1 \leq i \leq n$ *we have* $\lambda_i = e_\circ$.

A set $\{\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n\}$ *is a* basis of V *if* $\underline{v}_1, \ldots, \underline{v}_n$ *are linearly independent and each element can be represented as a linear combination of them, i.e.*

$$V = \left\{ \sum_{i=1}^{n} \lambda_i \odot \underline{v}_i \mid \lambda_i \in K \right\}.$$

The cardinality of the basis is the dimension of V*, denoted by* $\dim_K(V)$*. Note that the dimension can be infinite.*

An alternative definition of basis are that $\{\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n\}$ is a minimal set of generators, meaning that there are no fewer elements of V such that each element can be represented as a linear combination of them. Yet another definition states that a basis is a maximal set of linearly independent vectors.

Example Consider the vector space $\mathbb{R}^3$. The vectors $(1, 0, 0)$ and $(0, 1, 0)$ are linearly independent since

$$\lambda_1(1, 0, 0) + \lambda_2(0, 1, 0) = (\lambda_1, \lambda_2, 0) \stackrel{!}{=} (0, 0, 0)$$

forces $\lambda_1 = \lambda_2 = 0$. They do not form a basis since, e.g., the vector $(0, 0, 3)$ cannot be represented as a linear combination of them.

Since $2(1, 0, 0) = (2, 0, 0)$ the vectors $(1, 0, 0)$ and $(2, 0, 0)$ are linearly dependent.

The vectors $(1, 0, 0), (0, 1, 0)$, and $(1, 3, 0)$ are linearly dependent since a non-trivial linear combination is given by

$$(1, 0, 0) + 3(0, 1, 0) - (1, 3, 0) = (0, 0, 0).$$

The vectors $(1, 0, 0), (0, 1, 0)$, and $(0, 0, 1)$ are linearly independent and every other vector $(x, y, z) \in \mathbb{R}^3$ can be represented as a linear combination of them as

$$(x, y, z) = x(1, 0, 0) + y(0, 1, 0) + z(0, 0, 1).$$

So we have that a basis of $\mathbb{R}^3$ is given by $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ and that the dimension is $\dim_{\mathbb{R}}(\mathbb{R}^3) = 3$. In general $\dim_{\mathbb{R}}(\mathbb{R}^n) = n$.

Example We have already seen that the complex numbers form a vector space over the reals. A basis is given by $\{1, i\}$ and so the dimension is $\dim_{\mathbb{R}}(\mathbb{C}) = 2$.

Example Let K be a field and let $P_n \subset K[x]$ be the set of polynomials of degree at most n. A basis is given by $\{1, x, x^2, x^3, \ldots, x^n\}$ and so the dimension is $\dim_K(P_n) = n + 1$.

Alternative bases are easy to give. Since K is a field, x^i can be replaced by $a_i x^i$ for any nonzero $a_i \in K$, also linear combinations are possible. So another basis is given by $\{5, 3x - 1, -x^2, 2x^3 + x, \ldots, x^n + x^{n-1} + x^{n-2} + \cdots + x + 1\}$, since the degrees are all different and so none can be a linear combination of the others, while using linear algebra we can get every element as a linear combination.

Example $K[x]$ is a K vectorspace with $\dim_K(K[x]) = \infty$.