Лекція 15

ПИТАННЯ ДО ЗАЛІКУ ФМФ 29.12.2015

Питання 1. **Доведення алгоритму RSA.**

Питання 2. **Довести наступну теорему.**

Теорема 1. *Якщо* $a \equiv b \pmod{n}$, *то* $a^s \equiv b^s \pmod{n}$ *для будь-якого* $s \geq 1$.

Питання 3. **Довести наступну лему.**

Лема 1. *Нехай* n *є натуральним числом,* a k *та* j *є такими, що*

$$kj \equiv 1 \pmod{\phi(n)}, \tag{1}$$

тобто k *та* j *є оберненими за модулем* $\phi(n)$, *де* $\phi(n)$ — *це функція Ойлера. Якщо* $(a, n) = 1$, *то* $a^{kj} \equiv a \pmod{n}$.

Питання 4. **Довести наступну лему.**

Лема 2. *Нехай* $n = pq$, *де* p *та* q — *різні прості числа. Припустимо, що* k *та* j *є оберненими за модулем* $\phi(pq)$, ① *тобто виконано умову* (1). *Тоді*

$$a^{kj} \equiv a \pmod{pq} \quad \text{для всіх} \quad a. \tag{2}$$

Питання 5. **Довести наступну лему.**

---

[0] Printed from the file `[zalik.tex]` on 27.12.2015

[1] Згадайте, чому дорівнює $\phi(pq)$?

Лема 3. *Нехай p та q два різних простих числа. Якщо $c \equiv d \pmod{p}$ та $c \equiv d \pmod{q}$, то $c \equiv d \pmod{pq}$.*

Питання 6. Алгоритм швидкого піднесення у степінь.

Питання 7. Алгоритм швидкого піднесення у степінь за модулем.

Питання 8. Перевід числа у двійкову систему.

Питання 9. Довести наступну властивість.

Властивість 1. *Нехай p є простим числом, а $k \geq 1$. Тоді*

$$\phi\left(p^k\right) = p^k - p^{k-1}. \tag{3}$$

Питання 10. Довести наступну властивість.

Властивість 2. *Нехай p та q є різними простими числами. Тоді*

$$\phi\left(pq\right) = (p-1)(q-1). \tag{4}$$

Питання 11. Довести наступну властивість.

Властивість 3. *Нехай p та q є різними простими числами, а $i, j \geq 1$. Тоді*

$$\phi\left(p^i q^j\right) = (p^i - q^{i-1})(q^j - q^{j-1}). \tag{5}$$

Питання 12. Довести наступну властивість.

Властивість 4. *Нехай $p_1, \ldots, p_k$ — різні прості числа, а $i_1, \ldots, i_k \geq 1$. Тоді*

$$\phi\left(p_1^{i_1} \ldots p_k^{i_k}\right) = p_1^{i_1} \ldots p_k^{i_k} \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right). \tag{6}$$

Питання 13. Довести наступну властивість.

Властивість 5. *Нехай m та n є взаємно простими, тобто $(m,n)=1$. Тоді*

$$\phi(mn)=\phi(m)\,\phi(n)\,. \tag{7}$$

Питання 14. Довести наступну теорему.

Теорема 2 (*Л. Ойлер*). *Якщо $(a,m)=1$, то*

$$a^{\phi(m)} \equiv 1 \pmod{m}. \tag{8}$$

Питання 15. Довести наступну теорему.

Теорема 3 (*мала теорема Ферма*). *Якщо p є простим числом, то*

$$a^{p-1} \equiv 1 \pmod{p} \tag{9}$$

для будь-якого a, яке не ділиться на p.

Питання 16. Довести наступну теорему.

Теорема 4. *Рівняння*

$$ax \equiv b \pmod{m},$$

має єдиний розв'язок $0 \le x < m$ для довільного b тоді і тільки тоді, коли $(a,m)=1$.

Питання 17. Довести наступну теорему.

Теорема 5. *Система*

$$\begin{aligned} ax + by &\equiv e \pmod{m}, \\ cx + dy &\equiv f \pmod{m}. \end{aligned}$$

має єдиний розв'язок за модулем m тоді і тільки тоді, коли $(\Delta, m) = 1$, де $\Delta = ad - bc \pmod{m}$.

Питання 18. Довести наступну теорему.

Теорема 6 (*китайська теорема про остачі*). *Нехай $k \geq 1$ є натуральним числом. Нехай $m_1, \ldots, m_k$ є натуральними числами, які є попарно простими (не мають спільних дільників). Тоді система лінійних конгруенцій*

$$x \equiv a_i \pmod{m_i}, \qquad 1 \leq i \leq k,$$

має єдиний розв'язок за модулем $m_1 m_2 \ldots m_k$ для будь-яких натуральних $a_1, \ldots, a_k$.

Питання 19. Алгоритм знаходження частки та остачі від ділення.

Питання 20. Алгоритм Евкліда знаходження найбільшого спільного дільника.

Питання 21. Довести наступну лему.

Лема 4. *Якщо $i = jq + r$, $r \neq 0$, то $(i, j) = (j, r)$.*

Питання 22. Довести наступну теорему.

Теорема 7. *Рівняння*

$$ax + ny = 1$$

має розв'язок у цілих числах тоді і тільки тоді, коли

$$(a, n) = 1.$$

Якщо $(a, n) = 1$, *то для скорочення запису позначимо* $c = a^{-1} \pmod{n}$. *Тоді кожен розв'язок цього рівняння має вигляд*

$$x = c + \lambda n, \tag{10}$$

$$y = y_0 - a\lambda, \quad \text{де} \quad y_0 = \frac{1 - ac}{n} \tag{11}$$

при деякому $\lambda \in \mathbf{Z}$. ② *Один з розв'язків є таким, що*

$$x = a^{-1} \pmod{n}. \tag{12}$$

Питання 23. Побудова оберненого за модулем.

Питання 24. Довести наступну теорему.

Теорема 8 (*про існування оберненого за модулем***).** *Нехай* n *та* $1 \le a < n$ *є натуральними числами. Якщо* $(a, n) = 1$, *то* $a^{-1} \pmod{n}$ *існує. Якщо ж* $(a, n) \ne 1$, *то* $a^{-1} \pmod{n}$ *не існує.*

Питання 25. Довести наступний наслідок.

Наслідок 1. *Нехай* n *та* $1 \le a < n$ *є натуральними числами. Обернене* $a^{-1} \pmod{n}$ *існує тоді і тільки тоді, коли всі остачі* $ka \pmod{n}$, $1 \le k \le n$, *є різними.*

[2] Чому y_0 є цілим числом?

Питання 26. Довести наступну теорему.

Теорема 9. *Нехай $m \in \mathbf{Z}$, $n \in \mathbf{N}$. Тоді знайдуться такі два числа $q \in \mathbf{Z}$ та $0 \leq r < n$, що*

$$m = qn + r.$$

Таке представлення m через n є єдиним.

Питання 27. Довести наступну теорему.

Теорема 10. *Нехай $n \in \mathbf{N}$. Наступні три властивості виконуються для будь-яких $r, s, t \in \mathbf{Z}$.*

Властивість 6. $r \equiv r \pmod{n}$.

Властивість 7. $r \equiv s \pmod{n}$ *тоді і тільки тоді, коли* $s \equiv r \pmod{n}$.

Властивість 8. Якщо $r \equiv s \pmod{n}$ *і разом з цим* $s \equiv t \pmod{n}$, *то* $r \equiv t \pmod{n}$.

Питання 28. Довести наступну теорему.

Теорема 11 (*арифметичні властивості*). *Припустимо, що* $m_1 \equiv l_1 \pmod{n}$ *та* $m_2 \equiv l_2 \pmod{n}$. *Тоді*

Властивість 9. $m_1 + m_2 \equiv l_1 + l_2 \pmod{n}$;

Властивість 10. $m_1 - m_2 \equiv l_1 - l_2 \pmod{n}$;

Властивість 11. $m_1 m_2 \equiv l_1 l_2 \pmod{n}$.

Питання 29. Довести наступну теорему.

Теорема 12 (*основна теорема арифметики*). *Кожне натуральне число $n \geq 2$ розкладається у добуток простих чисел, причому цей розклад є єдиним з точністю до перестановки множників.*

Питання 30. Довести наступну теорему.

Теорема 13 (*необмеженість простих чисел*). *Нехай p — просте число. Тоді існує $p' > p$, яке також є простим.*