Задачи для подготовки к зачету по алгебре

Ноябрь, 2011

Приводятся примеры (относительно) типовых задач по основным темам зачета. Как обычно, на контрольной будут и (еще) более сложные задачи, предполагающие более тесное и творческое знакомство с материалом лекций.

Номера задач даны по книге Биркгофа–Барти.

1. Система RSA

1. (Первый из приславших правильное решение этой задачи получит 1 дополнительный балл к оценке за контрольную. При решении рекомендуется использовать компьютер.) Сообщение, состоящее из 11 букв русского алфавита (и составляющее хорошо известное слово), зашифровано следующим образом: буквы закодированы числами от 1 до 32 (по порядку в алфавите без Ё) и зашифрованы с помощью RSA. Известен один из параметров открытого ключа: e=11. Найдите недостающий параметр и расшифруйте сообщение:

643,692,182,692,182,692,48,180,1133,341,182.

2. В системе RSA с открытым ключем (187,7) зашифруйте 100 и расшифруйте 144.

3. В системе RSA с открытым ключем (143,7)

а) зашифруйте 2;

б) расшифруйте 142;

в) проверьте правильность обоих результатов с помощью обратного расшифровывания и шифрования.

2. Кольца

Задачи 10.2.6, 10.2.7, 11.2.7a, 10.2.9, 10.4.1, 10.7.3, 10.7.5, 10.7.9, 10.9.6, 10.9.7, 10.12.2a, 11.7.1, 11.7.2a.

4. Найдите порождающий элемент s идеала $I = \{r_1 f + r_2 g + r_3 h | r_1, r_2, r_3 \in R\}$, где R — кольцо многочленом над полем из 5 элементов, $f = 2\,x^4 + 3\,x^3 + x^2 + 4\,x, g = x^4 + 3\,x^3 + 4\,x^2 + 4\,x + 3, h = 3\,x^4 + 2\,x^3 + 4\,x^2 + x$.

3. Конечные поля

Задачи 10.9.7, 10.12.3, 11.2.3, 11.7.3,11.7.4,11.7.5, 11.7.6, 11.2.2, 12.5.2, 11.9.3*.

4. Приложения к арифметике

5. Найдите $\phi(10!)$.

6. Решите уравнения: а) $\phi(x) = 2$; б) $\phi(x) = 8$.

7. Найдите такое n, что число $2011^n - 1$ делится на 2012.

8. а) Опишите все такие целые числа x, которые дают остаток 5 от деления на 11, остаток 6 от деления на 15 и остаток 7 от деления на 32.

б) Опишите все такие многочлены $f = f(x)$ с рациональными коэффициентами, которые дают остаток x^n от деления на $x^{n+1} + 1$ при $n = 1, 2, 4$.