ФГБОУ ВПО «Пермский национальный
исследовательский политехнический университет»

Приложение теории чисел от ЕГЭ до современной криптографии

Грайфер Лазарь Борисович
к.ф.-м.н., доцент кафедры
Высшей математики ПНИПУ

Проект «Одаренные дети. Математика»

Актуальность

- Анализ заданий С6 по теории чисел в ЕГЭ позволяет убедиться в том, что базового курса математики достаточно для их решения.
- Защита информации в жизни играет все большую роль, особенно в связи с этапом модернизации в России, когда отношения гражданина и государства осуществляются в электронной форме.

Классы задач С6 ЕГЭ

- Делимость и признаки делимости.
- Десятичная запись числа.
- Целочисленные (диофантовые) уравнения, целочисленные неравенства.
- Числовые прогрессии.
- Текстовые задачи.

Метод RSA.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К
10	11	12	13	14	15	16	17	18	19	20

Л	М	Н	О	П	Р	С	Т	У	Ф	Х
21	22	23	24	25	26	27	28	29	30	31

Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
32	33	34	35	36	37	38	39	40	41

Рис 1. Таблица замены буквы на число.

«ФИЗМАТ» = 301817221028

Алгоритм шифрования

301817221028

- $p = 71;\ q = 107 => n = p * q = 7597$

3018 – 1722 – 1028

- $\varphi(n) = (p-1)(q-1) = 7420;\ e = 4947$

НОД $(\varphi(n), e) = 1$

- $E(3018) = 3018^{4947} mod\ 7597 = 4715$

$E(1722) = 1722^{4947} mod\ 7597 = 1764$

$E(1028) = 1028^{4947} mod\ 7597 = 1033$

- 471517641033

Алгоритм дешифрования

471517641033

- $\varphi(n) = 7420, e = 4947, n = 7597.$

4715 – 1764 – 1033

- $x * 4947 + y * 7420 = 1 => x = 3, y = -2$

$d = \varphi(n) + x = 7423$

- $D(4715) = 4715^{7423} mod\ 7597 = 3018$

$D(1764) = 1764^{7423} mod\ 7597 = 1722$

$D(1033) = 1033^{7423} mod\ 7597 = 1028$

- 301817221028

Эллиптические кривые

$$\frac{m(1+m)}{2} = \frac{n(n+1)(2n+1)}{6}$$

$$m = \frac{y-9}{18}, n = \frac{x-3}{6}$$

$$y^2 = x^3 - 9x + 81$$

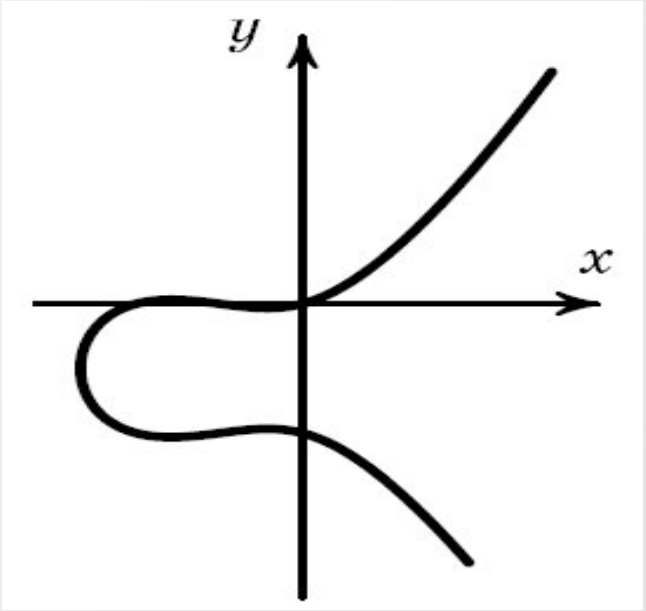

Рис 2. График кривой.

$$\frac{y(y+1)}{2} = \frac{x(x+1)(2x+1)}{6}$$

Сложение точек

- $P(x_p, y_p), Q(x_q, y_q), R(x_r, y_r)$

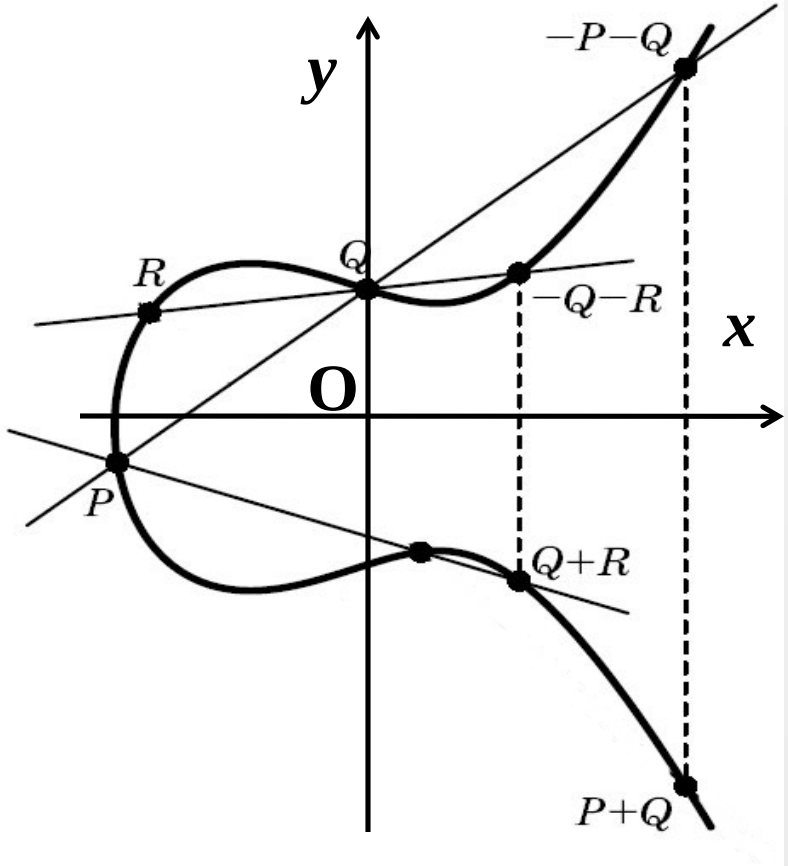

Рис 3. Сложение точек.

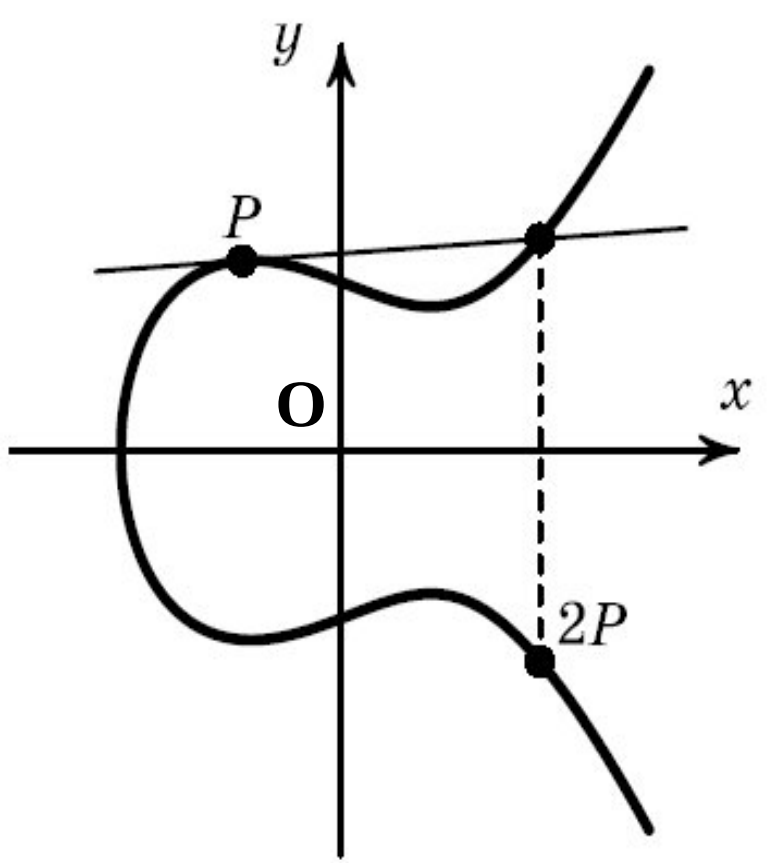

Рис 4. Удвоение точки.

Свойства суммы точек

- Коммутативность (P+Q=Q+P)
- Наличие нуля (P+0=0+P=P)
- Наличие противоположной точки ((-P)+P=0)
- Ассоциативность ((R+P)+Q=R+(P+Q))

На эллиптической кривой имеется точка $\infty = 0$, которая является точкой пересечения всех вертикалей.

Метод Эль-Гамаля

$$y^2 = x^3 - 9x + 81 \ (mod\ 149);$$

- Точка $B(0; 9)$ – точка-“основания”.
- Точка $P(9; 27)$ – сообщение.
- Отправитель: k=100; Получатель: n=250.

Шифрование

- kB=100B $= 2 * 2 * (2 * 2 * 2(B + 2B) + B)$; 100B(66;3)
- nB=250B; 250B (64;68)
- k(nB)=100*(250B); 100*(250B) (69;13)
- P(9;27), 100*250B (69;13); P+k(nB) (104;20)
- Отправитель посылает пару точек: ((66;3); (104;20))

Дешифрование

- ((66;3); (104;20))
- n(kB) = 250*(100B); n(kB) (69;13)
- -n(kB) (69;136)
- P+n(kB)-n(kB) = P; P (9;27).

Заключение

- Методами, являющимися развитием идей школьной программы о натуральных числах, решаются несколько задач криптографии открытых ключей с небольшим временем шифрования, но с относительно высоким уровнем криптозащиты.