

Κρυπτογραφία

Έλεγχος πρώτων αριθμών-Παραγοντοποίηση

Διαφάνειες: Άρης Παγουρτζής – Πέτρος Ποτίκας

Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Εισαγωγή

- ▶ **Παραγοντοποίηση**: Δίνεται ένας σύνθετος αριθμός N , θέλουμε βρούμε θετικούς ακεραίους p, q , τ.ώ. $N = pq$

Εισαγωγή

- ▶ **Παραγοντοποίηση**: Δίνεται ένας σύνθετος αριθμός N , θέλουμε βρούμε θετικούς ακεραίους p, q , τ.ώ. $N = pq$
- ▶ Υπολογιστικά δύσκολο πρόβλημα θεωρίας αριθμών

Εισαγωγή

- ▶ **Παραγοντοποίηση**: Δίνεται ένας σύνθετος αριθμός N , θέλουμε βρούμε θετικούς ακεραίους p, q , τ.ώ. $N = pq$
- ▶ Υπολογιστικά δύσκολο πρόβλημα θεωρίας αριθμών
- ▶ Μπορεί να λυθεί *δοκιμάζοντας διαιρέσεις* (διαιρώντας με όλους τους περιττούς από 2 έως \sqrt{N})

Εισαγωγή

- ▶ **Παραγοντοποίηση**: Δίνεται ένας σύνθετος αριθμός N , θέλουμε βρούμε θετικούς ακεραίους p, q , τ.ώ. $N = pq$
- ▶ Υπολογιστικά δύσκολο πρόβλημα θεωρίας αριθμών
- ▶ Μπορεί να λυθεί *δοκιμάζοντας διαιρέσεις* (διαιρώντας με όλους τους περιττούς από 2 έως \sqrt{N})
- ▶ Εκθετικός χρόνος ως προς το μήκος του N (\sqrt{N} διαιρέσεις, χρόνου $(\log(N))^c$, για κάποια σταθερά c)

Εισαγωγή

- ▶ **Παραγοντοποίηση:** Δίνεται ένας σύνθετος αριθμός N , θέλουμε βρούμε θετικούς ακεραίους p, q , τ.ώ. $N = pq$
- ▶ Υπολογιστικά δύσκολο πρόβλημα θεωρίας αριθμών
- ▶ Μπορεί να λυθεί δοκιμάζοντας διαιρέσεις (διαιρώντας με όλους τους περιττούς από 2 έως \sqrt{N})
- ▶ Εκθετικός χρόνος ως προς το μήκος του N (\sqrt{N} διαιρέσεις, χρόνου $(\log(N))^c$, για κάποια σταθερά c)
- ▶ Στην κρυπτογραφία, οι αριθμοί που είναι γινόμενο μεγάλων πρώτων αριθμών είναι ποιο δύσκολο να παραγοντοποιηθούν

Εισαγωγή

- ▶ **Παραγοντοποίηση:** Δίνεται ένας σύνθετος αριθμός N , θέλουμε βρούμε θετικούς ακεραίους p, q , τ.ώ. $N = pq$
- ▶ Υπολογιστικά δύσκολο πρόβλημα θεωρίας αριθμών
- ▶ Μπορεί να λυθεί *δοκιμάζοντας διαιρέσεις* (διαιρώντας με όλους τους περιττούς από 2 έως \sqrt{N})
- ▶ Εκθετικός χρόνος ως προς το μήκος του N (\sqrt{N} διαιρέσεις, χρόνου $(\log(N))^c$, για κάποια σταθερά c)
- ▶ Στην κρυπτογραφία, οι αριθμοί που είναι γινόμενο μεγάλων πρώτων αριθμών είναι ποιο δύσκολο να παραγοντοποιηθούν
- ▶ Θέλουμε να παράγουμε *αποδοτικά* δύο n -bit μεγάλους πρώτους, ώστε $N = pq$

Εισαγωγή

- ▶ **Παραγοντοποίηση:** Δίνεται ένας σύνθετος αριθμός N , θέλουμε βρούμε θετικούς ακεραίους p, q , τ.ώ. $N = pq$
- ▶ Υπολογιστικά δύσκολο πρόβλημα θεωρίας αριθμών
- ▶ Μπορεί να λυθεί *δοκιμάζοντας διαιρέσεις* (διαιρώντας με όλους τους περιττούς από 2 έως \sqrt{N})
- ▶ Εκθετικός χρόνος ως προς το μήκος του N (\sqrt{N} διαιρέσεις, χρόνου $(\log(N))^c$, για κάποια σταθερά c)
- ▶ Στην κρυπτογραφία, οι αριθμοί που είναι γινόμενο μεγάλων πρώτων αριθμών είναι ποιο δύσκολο να παραγοντοποιηθούν
- ▶ Θέλουμε να παράγουμε *αποδοτικά* δύο n -bit μεγάλους πρώτους, ώστε $N = pq$
- ▶ **Primality:** έλεγχος αν ένας αριθμός είναι πρώτος (εύκολο υπολογιστικά)

Εισαγωγή

- ▶ **Παραγοντοποίηση:** Δίνεται ένας σύνθετος αριθμός N , θέλουμε βρούμε θετικούς ακεραίους p, q , τ.ώ. $N = pq$
- ▶ Υπολογιστικά δύσκολο πρόβλημα θεωρίας αριθμών
- ▶ Μπορεί να λυθεί *δοκιμάζοντας διαιρέσεις* (διαιρώντας με όλους τους περιττούς από 2 έως \sqrt{N})
- ▶ Εκθετικός χρόνος ως προς το μήκος του N (\sqrt{N} διαιρέσεις, χρόνου $(\log(N))^c$, για κάποια σταθερά c)
- ▶ Στην κρυπτογραφία, οι αριθμοί που είναι γινόμενο μεγάλων πρώτων αριθμών είναι ποιο δύσκολο να παραγοντοποιηθούν
- ▶ Θέλουμε να παράγουμε *αποδοτικά* δύο n -bit μεγάλους πρώτους, ώστε $N = pq$
- ▶ **Primality:** έλεγχος αν ένας αριθμός είναι πρώτος (εύκολο υπολογιστικά)
- ▶ Κόσκινο Ερατοσθένη

Εισαγωγή

- ▶ **Παραγοντοποίηση:** Δίνεται ένας σύνθετος αριθμός N , θέλουμε βρούμε θετικούς ακεραίους p, q , τ.ώ. $N = pq$
- ▶ Υπολογιστικά δύσκολο πρόβλημα θεωρίας αριθμών
- ▶ Μπορεί να λυθεί *δοκιμάζοντας διαιρέσεις* (διαιρώντας με όλους τους περιττούς από 2 έως \sqrt{N})
- ▶ Εκθετικός χρόνος ως προς το μήκος του N (\sqrt{N} διαιρέσεις, χρόνου $(\log(N))^c$, για κάποια σταθερά c)
- ▶ Στην κρυπτογραφία, οι αριθμοί που είναι γινόμενο μεγάλων πρώτων αριθμών είναι ποιο δύσκολο να παραγοντοποιηθούν
- ▶ Θέλουμε να παράγουμε *αποδοτικά* δύο n -bit μεγάλους πρώτους, ώστε $N = pq$
- ▶ **Primality:** έλεγχος αν ένας αριθμός είναι πρώτος (εύκολο υπολογιστικά)
- ▶ Κόσκινο Ερατοσθένη (εκθετικό)

Παραγωγή τυχαίου πρώτου αριθμού

Αλγόριθμος παραγωγής τυχαίου πρώτου μήκους n -bits

Είσοδος: μήκος n ; παράμετρος t

Έξοδος: Ένας τυχαίος n -bit πρώτος

for $i = 1$ to t **do** :

$p' \leftarrow \{0, 1\}^{n-1}$

$p := 1 || p'$

if p is prime return p

return fail

Εισαγωγή

- ▶ $\pi(N)$: το πλήθος των πρώτων που είναι μικρότεροι ή ίσοι με το N

Εισαγωγή

- ▶ $\pi(N)$: το πλήθος των πρώτων που είναι μικρότεροι ή ίσοι με το N
- ▶ Από **θεώρημα πρώτων αριθμών**: $\pi(N) \approx N/\ln N$

Εισαγωγή

- ▶ $\pi(N)$: το πλήθος των πρώτων που είναι μικρότεροι ή ίσοι με το N
- ▶ Από **θεώρημα πρώτων αριθμών**: $\pi(N) \approx N/\ln N$
- ▶ Αν ένας ακέραιος p επιλεγεί τυχαία από το 1 ως το N , τότε η πιθανότητα να είναι πρώτος είναι $1/\ln N$

Εισαγωγή

- ▶ $\pi(N)$: το πλήθος των πρώτων που είναι μικρότεροι ή ίσοι με το N
- ▶ Από **θεώρημα πρώτων αριθμών**: $\pi(N) \approx N/\ln N$
- ▶ Αν ένας ακέραιος p επιλεγεί τυχαία από το 1 ως το N , τότε η πιθανότητα να είναι πρώτος είναι $1/\ln N$
- ▶ Έστω πως n είναι ακέραιος 1024-bits και $n = pq$, με p, q πρώτους, μήκους 512-bits. Η πιθανότητα ενός τυχαίου ακεραίου 512-bits να είναι πρώτος είναι $1/355$ (ή $2/355$, αν πάρω περιττό)

Εισαγωγή

- ▶ $\pi(N)$: το πλήθος των πρώτων που είναι μικρότεροι ή ίσοι με το N
- ▶ Από **θεώρημα πρώτων αριθμών**: $\pi(N) \approx N/\ln N$
- ▶ Αν ένας ακέραιος p επιλεγεί τυχαία από το 1 ως το N , τότε η πιθανότητα να είναι πρώτος είναι $1/\ln N$
- ▶ Έστω πως n είναι ακέραιος 1024-bits και $n = pq$, με p, q πρώτους, μήκους 512-bits. Η πιθανότητα ενός τυχαίου ακεραίου 512-bits να είναι πρώτος είναι $1/355$ (ή $2/355$, αν πάρω περιττό)
- ▶ Συμπέρασμα: μπορώ να κατασκευάσω πρώτους p, q και $n = pq$ (RSA)

Εισαγωγή

- ▶ $\pi(N)$: το πλήθος των πρώτων που είναι μικρότεροι ή ίσοι με το N
- ▶ Από **θεώρημα πρώτων αριθμών**: $\pi(N) \approx N/\ln N$
- ▶ Αν ένας ακέραιος p επιλεγεί τυχαία από το 1 ως το N , τότε η πιθανότητα να είναι πρώτος είναι $1/\ln N$
- ▶ Έστω πως n είναι ακέραιος 1024-bits και $n = pq$, με p, q πρώτους, μήκους 512-bits. Η πιθανότητα ενός τυχαίου ακεραίου 512-bits να είναι πρώτος είναι $1/355$ (ή $2/355$, αν πάρω περιττό)
- ▶ Συμπέρασμα: μπορώ να κατασκευάσω πρώτους p, q και $n = pq$ (RSA)
- ▶ Έλεγχος αν ένας αριθμός είναι πρώτος

Έλεγχος αν ένας αριθμός είναι πρώτος

- ▶ Το 1970 αναπτύχθηκαν οι πρώτοι αποδοτικοί *πιθανοτικοί* αλγόριθμοι.

Έλεγχος αν ένας αριθμός είναι πρώτος

- ▶ Το 1970 αναπτύχθηκαν οι πρώτοι αποδοτικοί *πιθανοτικοί* αλγόριθμοι.
- ▶ Ιδιότητα: Αν η είσοδος p είναι πρώτος, τότε η έξοδος είναι πάντα “πρώτος”. Αν ο p είναι σύνθετος, τότε η έξοδος είναι “σύνθετος” με μεγάλη πιθανότητα.

Έλεγχος αν ένας αριθμός είναι πρώτος

- ▶ Το 1970 αναπτύχθηκαν οι πρώτοι αποδοτικοί *πιθανοτικοί* αλγόριθμοι.
- ▶ Ιδιότητα: Αν η είσοδος p είναι πρώτος, τότε η έξοδος είναι πάντα “πρώτος”. Αν ο p είναι σύνθετος, τότε η έξοδος είναι “σύνθετος” με μεγάλη πιθανότητα.
- ▶ Ισοδύναμα, αν η έξοδος είναι “σύνθετος” (?)

Έλεγχος αν ένας αριθμός είναι πρώτος

- ▶ Το 1970 αναπτύχθηκαν οι πρώτοι αποδοτικοί *πιθανοτικοί* αλγόριθμοι.
- ▶ Ιδιότητα: Αν η είσοδος p είναι πρώτος, τότε η έξοδος είναι πάντα “πρώτος”. Αν ο p είναι σύνθετος, τότε η έξοδος είναι “σύνθετος” με μεγάλη πιθανότητα.
- ▶ Ισοδύναμα, αν η έξοδος είναι “σύνθετος” (?), τότε σίγουρα είναι σύνθετος, ενώ αν είναι “πρώτος” (?)

Έλεγχος αν ένας αριθμός είναι πρώτος

- ▶ Το 1970 αναπτύχθηκαν οι πρώτοι αποδοτικοί *πιθανοτικοί* αλγόριθμοι.
- ▶ Ιδιότητα: Αν η είσοδος p είναι πρώτος, τότε η έξοδος είναι πάντα “πρώτος”. Αν ο p είναι σύνθετος, τότε η έξοδος είναι “σύνθετος” με μεγάλη πιθανότητα.
- ▶ Ισοδύναμα, αν η έξοδος είναι “σύνθετος” (?), τότε σίγουρα είναι σύνθετος, ενώ αν είναι “πρώτος” (?), τότε πολύ πιθανά να είναι πρώτος.

Fermat (primality) test

Έλεγχος Fermat

Για να δούμε αν ένας δοσμένος ακέραιος n είναι πρώτος:

Επιλέγουμε τυχαία $a \in \mathbb{Z}_n$: αν $a^{n-1} \not\equiv 1 \pmod{n}$ τότε n σύνθετος (με βεβαιότητα), αλλιώς λέμε ότι το n περνάει το test (ίσως είναι πρώτος). Στην δεύτερη περίπτωση επαναλαμβάνουμε.

Πρόταση.

Αν για σύνθετο n υπάρχει ένας **μάρτυρας (witness)** (δηλ. $a \in \mathbb{Z}_n$, $a^{n-1} \not\equiv 1 \pmod{n}$), τότε υπάρχουν τουλάχιστον $n/2$ μάρτυρες.

Απόδειξη. Χρήση Θ . Lagrange στην ομάδα των **μη μαρτύρων** του $U(\mathbb{Z}_n)$.

Πόρισμα: ο έλεγχος Fermat απαντάει σωστά με πολύ μεγάλη πιθανότητα για τους περισσότερους αριθμούς. Εξαιρούνται όμως οι **αριθμοί Carmichael**: σύνθετοι για τους οποίους δεν υπάρχει μάρτυρας Fermat. Για να καλύψουμε και αυτούς: **Miller-Rabin test**.

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \dots, n - 1]$. Αν $b^{n-1} \bmod n \neq 1$, τότε το n **δεν περνάει** τον έλεγχο (είναι **σίγουρα σύνθετος**).

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \dots, n - 1]$. Αν $b^{n-1} \bmod n \neq 1$, τότε το n **δεν περνάει** τον έλεγχο (είναι **σίγουρα σύνθετος**).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \dots, n - 1]$. Αν $b^{n-1} \bmod n \neq 1$, τότε το n **δεν περνάει** τον έλεγχο (είναι **σίγουρα σύνθετος**).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.
4. Αν $b^t \equiv \pm 1 \pmod{n}$, τότε το n **περνάει** τον έλεγχο (**πιθανόν πρώτος**).

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \dots, n - 1]$. Αν $b^{n-1} \bmod n \neq 1$, τότε το n **δεν περνάει** τον έλεγχο (είναι **σίγουρα σύνθετος**).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.
4. Αν $b^t \equiv \pm 1 \pmod{n}$, τότε το n **περνάει** τον έλεγχο (**πιθανόν πρώτος**).
5. Αλλιώς, υψώνουμε το $b^t \bmod n$ στο τετράγωνο: $b^{2t} \bmod n$, έπειτα ξανά στο τετράγωνο $\bmod n$ κ.ο.κ. έως ότου πάρουμε ± 1 (το πολύ $s - 1$ επαναλήψεις).

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \dots, n - 1]$. Αν $b^{n-1} \bmod n \neq 1$, τότε το n **δεν περνάει** τον έλεγχο (είναι **σίγουρα σύνθετος**).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.
4. Αν $b^t \equiv \pm 1 \pmod{n}$, τότε το n **περνάει** τον έλεγχο (**πιθανόν πρώτος**).
5. Αλλιώς, υψώνουμε το $b^t \bmod n$ στο τετράγωνο: $b^{2^i t} \bmod n$, έπειτα ξανά στο τετράγωνο $\bmod n$ κ.ο.κ. έως ότου πάρουμε ± 1 (το πολύ $s - 1$ επαναλήψεις).
6. Αν πάρουμε **πρώτα** -1 τότε το n **περνάει** τον έλεγχο (πιθανόν πρώτος), **αλλιώς δεν περνάει** τον έλεγχο (σίγουρα σύνθετος).

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \dots, n - 1]$. Αν $b^{n-1} \bmod n \neq 1$, τότε το n **δεν περνάει** τον έλεγχο (είναι **σίγουρα σύνθετος**).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.
4. Αν $b^t \equiv \pm 1 \pmod{n}$, τότε το n **περνάει** τον έλεγχο (**πιθανόν πρώτος**).
5. Αλλιώς, υψώνουμε το $b^t \bmod n$ στο τετράγωνο: $b^{2t} \bmod n$, έπειτα ξανά στο τετράγωνο $\bmod n$ κ.ο.κ. έως ότου πάρουμε ± 1 (το πολύ $s - 1$ επαναλήψεις).
6. Αν πάρουμε **πρώτα** -1 τότε το n **περνάει** τον έλεγχο (πιθανόν πρώτος), **αλλιώς δεν περνάει** τον έλεγχο (σίγουρα σύνθετος).

Ορθότητα: Θα αποδείξουμε ότι η πιθανότητα αποτυχίας είναι $< \frac{1}{2}$.

Έλεγχος πρώτων αριθμών Miller-Rabin

1. Έστω $n \in \mathbb{Z}$ θετικός περιττός αριθμός.
2. Επιλέγουμε τυχαία $b \in [2, \dots, n - 1]$. Αν $b^{n-1} \bmod n \neq 1$, τότε το n **δεν περνάει** τον έλεγχο (είναι **σίγουρα σύνθετος**).
3. Αλλιώς, γράφουμε $n - 1 = 2^s t$, με t περιττό.
4. Αν $b^t \equiv \pm 1 \pmod{n}$, τότε το n **περνάει** τον έλεγχο (**πιθανόν πρώτος**).
5. Αλλιώς, υψώνουμε το $b^t \bmod n$ στο τετράγωνο: $b^{2t} \bmod n$, έπειτα ξανά στο τετράγωνο $\bmod n$ κ.ο.κ. έως ότου πάρουμε ± 1 (το πολύ $s - 1$ επαναλήψεις).
6. Αν πάρουμε **πρώτα** -1 τότε το n **περνάει** τον έλεγχο (πιθανόν πρώτος), **αλλιώς δεν περνάει** τον έλεγχο (σίγουρα σύνθετος).

Ορθότητα: Θα αποδείξουμε ότι η πιθανότητα αποτυχίας είναι $< \frac{1}{2}$.

Μπορεί να γίνει *αμελητέα* (*negligible*) με **επαναλήψεις του ελέγχου για άλλο b κάθε φορά**.

Έλεγχος πρώτων αριθμών Miller-Rabin: ορθότητα

Πρόταση

Αν n πρώτος, τότε περνάει τον έλεγχο πάντοτε (για όλα τα b). Αν n σύνθετος τότε περνάει τον έλεγχο για λιγότερα από τα μισά b .

Έλεγχος πρώτων αριθμών Miller-Rabin: ορθότητα

Πρόταση

Αν n πρώτος, τότε περνάει τον έλεγχο πάντοτε (για όλα τα b). Αν n σύνθετος τότε περνάει τον έλεγχο για *λιγότερα από τα μισά* b .

Απόδειξη.

Βασίζεται στην απεικόνιση $b \mapsto \langle b^t, b^{2t}, \dots, b^{2^i t}, \dots, b^{2^s t} \rangle \pmod{n}$.

Έλεγχος πρώτων αριθμών Miller-Rabin: ορθότητα

Πρόταση

Αν n πρώτος, τότε περνάει τον έλεγχο πάντοτε (για όλα τα b). Αν n σύνθετος τότε περνάει τον έλεγχο για *λιγότερα από τα μισά* b .

Απόδειξη.

Βασίζεται στην απεικόνιση $b \mapsto \langle b^t, b^{2t}, \dots, b^{2^i t}, \dots, b^{2^s t} \rangle \pmod{n}$.

Factoring sequence: $\langle \not\equiv \pm 1, \dots, \not\equiv \pm 1, \equiv 1, \dots, \equiv 1 \rangle \pmod{n}$.

Έλεγχος πρώτων αριθμών Miller-Rabin: ορθότητα

Πρόταση

Αν n πρώτος, τότε περνάει τον έλεγχο πάντοτε (για όλα τα b). Αν n σύνθετος τότε περνάει τον έλεγχο για *λιγότερα από τα μισά* b .

Απόδειξη.

Βασίζεται στην απεικόνιση $b \mapsto \langle b^t, b^{2t}, \dots, b^{2^i t}, \dots, b^{2^s t} \rangle \pmod{n}$.

Factoring sequence: $\langle \not\equiv \pm 1, \dots, \not\equiv \pm 1, \equiv 1, \dots, \equiv 1 \rangle \pmod{n}$.

Αποδεικνύεται με χρήση του Θ. Lagrange ότι τα στοιχεία που απεικονίζονται σε non-factoring sequences είναι το πολύ τα μισά.

Λεπτομέρειες: στον πίνακα. □

Ντετερμινιστικός έλεγχος πρώτων

Αλγόριθμος AKS (2002) είναι ντετερμινιστικός, αλλά αργός ($O(n^{5+\epsilon})$) για αυτό πρακτικά χρησιμοποιούνται οι πιθανοτικοί αλγόριθμοι

Παραγοντοποίηση Pollard rho

- ▶ Έστω p ο μικρότερος πρώτος διαιρέτης του n . Ψάχνουμε $x \neq x' \in \mathbb{Z}_n$, τ.ώ. $x \equiv x' \pmod{p}$

Παραγοντοποίηση Pollard rho

- ▶ Έστω p ο μικρότερος πρώτος διαιρέτης του n . Ψάχνουμε $x \neq x' \in \mathbb{Z}_n$, τ.ώ. $x \equiv x' \pmod{p}$
- ▶ Τότε από $\gcd(x - x', n)$, μπορεί να προκύψει μη τετριμμένος διαιρέτης του n (p άγνωστο!).

Παραγοντοποίηση Pollard rho

- ▶ Έστω p ο μικρότερος πρώτος διαιρέτης του n . Ψάχνουμε $x \neq x' \in \mathbb{Z}_n$, τ.ώ. $x \equiv x' \pmod{p}$
- ▶ Τότε από $\gcd(x - x', n)$, μπορεί να προκύψει μη τετριμμένος διαιρέτης του n (p άγνωστο!).
- ▶ Επιλέγουμε τυχαίο $X \subseteq \mathbb{Z}_n$ και υπολογίζουμε για όλα τα x, x' το $\gcd(x - x', n)$

Παραγοντοποίηση Pollard rho

- ▶ Έστω p ο μικρότερος πρώτος διαιρέτης του n . Ψάχνουμε $x \neq x' \in \mathbb{Z}_n$, τ.ώ. $x \equiv x' \pmod{p}$
- ▶ Τότε από $\gcd(x - x', n)$, μπορεί να προκύψει μη τετριμμένος διαιρέτης του n (p άγνωστο!).
- ▶ Επιλέγουμε τυχαίο $X \subseteq \mathbb{Z}_n$ και υπολογίζουμε για όλα τα x, x' το $\gcd(x - x', n)$
- ▶ Από παράδοξο γενεθλίων, πρέπει $|X| \approx 1.17\sqrt{n}$ για να έχουμε σύγκρουση με πιθανότητα 50%.

Παραγοντοποίηση Pollard rho

- ▶ Έστω p ο μικρότερος πρώτος διαιρέτης του n . Ψάχνουμε $x \neq x' \in \mathbb{Z}_n$, τ.ώ. $x \equiv x' \pmod{p}$
- ▶ Τότε από $\gcd(x - x', n)$, μπορεί να προκύψει μη τετριμμένος διαιρέτης του n (p άγνωστο!).
- ▶ Επιλέγουμε τυχαίο $X \subseteq \mathbb{Z}_n$ και υπολογίζουμε για όλα τα x, x' το $\gcd(x - x', n)$
- ▶ Από παράδοξο γενεθλίων, πρέπει $|X| \approx 1.17\sqrt{n}$ για να έχουμε σύγκρουση με πιθανότητα 50%.
- ▶ Για να το κάνουμε αυτό θέλουμε όλα τα $\gcd(x - x', n)$ (αφού p άγνωστο, αδύνατος ο υπολογισμός των $x \pmod{p}$ και μετά ταξινόμηση), άρα $\binom{|X|}{2} > p/2$ δοκιμές

Παραγοντοποίηση Pollard rho

- ▶ Θεωρούμε f πολυώνυμο με ακέραιους συντελεστές, π.χ. $f(x) = x^2 + 1$
- ▶ Έστω $x_1 \in \mathbb{Z}_n$ και x_1, x_2, \dots , όπου $x_j = f(x_{j-1})$, $j \geq 2$. Η f παράγει σχεδόν τυχαία στοιχεία.
- ▶ Για να έχω $\gcd(x_j - x_i, n)$, πρέπει για κάθε νέο x_j , να υπολογίζω τα $\gcd(x_i - x_j, n)$, για όλα $i < j$.

Παραγοντοποίηση Pollard rho

- ▶ Θεωρούμε f πολυώνυμο με ακέραιους συντελεστές, π.χ. $f(x) = x^2 + 1$
- ▶ Έστω $x_1 \in \mathbb{Z}_n$ και x_1, x_2, \dots , όπου $x_j = f(x_{j-1})$, $j \geq 2$. Η f παράγει σχεδόν τυχαία στοιχεία.
- ▶ Για να έχω $\gcd(x_j - x_i, n)$, πρέπει για κάθε νέο x_j , να υπολογίζω τα $\gcd(x_i - x_j, n)$, για όλα $i < j$. Τετραγωνικό!

Παραγοντοποίηση Pollard rho

- ▶ Καλύτερο: Αν $x_i \bmod p = x_j \bmod p$, τότε $x_{i+1} \bmod p = x_{j+1} \bmod p$ (λόγω της f και $p|n$)

Παραγοντοποίηση Pollard rho

- ▶ Καλύτερο: Αν $x_i \bmod p = x_j \bmod p$, τότε $x_{i+1} \bmod p = x_{j+1} \bmod p$ (λόγω της f και $p|n$)
- ▶ Επαναλαμβάνοντας, αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i+\delta} \equiv x_{j+\delta} \pmod{p}$, $\delta \geq 0$

Παραγοντοποίηση Pollard rho

- ▶ Καλύτερο: Αν $x_i \bmod p = x_j \bmod p$, τότε $x_{i+1} \bmod p = x_{j+1} \bmod p$ (λόγω της f και $p|n$)
- ▶ Επαναλαμβάνοντας, αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i+\delta} \equiv x_{j+\delta} \pmod{p}$, $\delta \geq 0$
- ▶ Θεωρώντας $l = j - i$, έχουμε ότι: $x_{i'} \equiv x_{j'} \pmod{p}$, αν $j' > i' \geq i$ και $j' - i' \equiv 0 \pmod{l}$

Παραγοντοποίηση Pollard rho

- ▶ Καλύτερο: Αν $x_i \bmod p = x_j \bmod p$, τότε $x_{i+1} \bmod p = x_{j+1} \bmod p$ (λόγω της f και $p|n$)
- ▶ Επαναλαμβάνοντας, αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i+\delta} \equiv x_{j+\delta} \pmod{p}$, $\delta \geq 0$
- ▶ Θεωρώντας $l = j - i$, έχουμε ότι: $x_{i'} \equiv x_{j'} \pmod{p}$, αν $j' > i' \geq i$ και $j' - i' \equiv 0 \pmod{l}$
- ▶ Γράφος G : κορυφές τα x_i , κατευθυνόμενες ακμές από το $x_i \bmod p$ στο $x_{i+1} \bmod p$.

Παραγοντοποίηση Pollard rho

- ▶ Καλύτερο: Αν $x_i \bmod p = x_j \bmod p$, τότε $x_{i+1} \bmod p = x_{j+1} \bmod p$ (λόγω της f και $p|n$)
- ▶ Επαναλαμβάνοντας, αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i+\delta} \equiv x_{j+\delta} \pmod{p}$, $\delta \geq 0$
- ▶ Θεωρώντας $l = j - i$, έχουμε ότι: $x_{i'} \equiv x_{j'} \pmod{p}$, αν $j' > i' \geq i$ και $j' - i' \equiv 0 \pmod{l}$
- ▶ Γράφος G : κορυφές τα x_i , κατευθυνόμενες ακμές από το $x_i \bmod p$ στο $x_{i+1} \bmod p$.
- ▶ Πρέπει να υπάρχει ένα πρώτο ζευγάρι x_i, x_j , με $i < j$ ώστε $x_i \equiv x_j \pmod{p}$,

Παραγοντοποίηση Pollard rho

- ▶ Καλύτερο: Αν $x_i \bmod p = x_j \bmod p$, τότε $x_{i+1} \bmod p = x_{j+1} \bmod p$ (λόγω της f και $p|n$)
- ▶ Επαναλαμβάνοντας, αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i+\delta} \equiv x_{j+\delta} \pmod{p}$, $\delta \geq 0$
- ▶ Θεωρώντας $l = j - i$, έχουμε ότι: $x_{i'} \equiv x_{j'} \pmod{p}$, αν $j' > i' \geq i$ και $j' - i' \equiv 0 \pmod{l}$
- ▶ Γράφος G : κορυφές τα x_i , κατευθυνόμενες ακμές από το $x_i \bmod p$ στο $x_{i+1} \bmod p$.
- ▶ Πρέπει να υπάρχει ένα πρώτο ζευγάρι x_i, x_j , με $i < j$ ώστε $x_i \equiv x_j \pmod{p}$,
 $x_1 \bmod p \rightarrow x_2 \bmod p \cdots \rightarrow x_i \bmod p$ (ουρά)

Παραγοντοποίηση Pollard rho

- ▶ Καλύτερο: Αν $x_i \bmod p = x_j \bmod p$, τότε $x_{i+1} \bmod p = x_{j+1} \bmod p$ (λόγω της f και $p|n$)
- ▶ Επαναλαμβάνοντας, αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i+\delta} \equiv x_{j+\delta} \pmod{p}$, $\delta \geq 0$
- ▶ Θεωρώντας $l = j - i$, έχουμε ότι: $x_{i'} \equiv x_{j'} \pmod{p}$, αν $j' > i' \geq i$ και $j' - i' \equiv 0 \pmod{l}$
- ▶ Γράφος G : κορυφές τα x_i , κατευθυνόμενες ακμές από το $x_i \bmod p$ στο $x_{i+1} \bmod p$.
- ▶ Πρέπει να υπάρχει ένα πρώτο ζευγάρι x_i, x_j , με $i < j$ ώστε $x_i \equiv x_j \pmod{p}$,
 $x_1 \bmod p \rightarrow x_2 \bmod p \cdots \rightarrow x_i \bmod p$ (ουρά)
 $x_i \bmod p \rightarrow x_{i+1} \bmod p \cdots \rightarrow x_j \bmod p \equiv x_i \bmod p$ (κύκλος)

Παραγοντοποίηση Pollard rho

- ▶ Καλύτερο: Αν $x_i \bmod p = x_j \bmod p$, τότε $x_{i+1} \bmod p = x_{j+1} \bmod p$ (λόγω της f και $p|n$)
- ▶ Επαναλαμβάνοντας, αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i+\delta} \equiv x_{j+\delta} \pmod{p}$, $\delta \geq 0$
- ▶ Θεωρώντας $l = j - i$, έχουμε ότι: $x_{i'} \equiv x_{j'} \pmod{p}$, αν $j' > i' \geq i$ και $j' - i' \equiv 0 \pmod{l}$
- ▶ Γράφος G : κορυφές τα x_i , κατευθυνόμενες ακμές από το $x_i \bmod p$ στο $x_{i+1} \bmod p$.
- ▶ Πρέπει να υπάρχει ένα πρώτο ζευγάρι x_i, x_j , με $i < j$ ώστε $x_i \equiv x_j \pmod{p}$,
 $x_1 \bmod p \rightarrow x_2 \bmod p \cdots \rightarrow x_i \bmod p$ (ουρά)
 $x_i \bmod p \rightarrow x_{i+1} \bmod p \cdots \rightarrow x_j \bmod p \equiv x_i \bmod p$ (κύκλος)
- ▶ Από τη μορφή του γράφου, το όνομα της μεθόδου (ρ).

Παραγοντοποίηση Pollard rho

- ▶ Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αλλά παίρνουμε $j = 2i$

Παραγοντοποίηση Pollard rho

- ▶ Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αλλά παίρνουμε $j = 2i$
- ▶ Αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i'} \equiv x_{2i'} \pmod{p}$, για όλα τα $i' \equiv 0 \pmod{l}$, $i' \geq i$

Παραγοντοποίηση Pollard rho

- ▶ Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αλλά παίρνουμε $j = 2i$
- ▶ Αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i'} \equiv x_{2i'} \pmod{p}$, για όλα τα $i' \equiv 0 \pmod{l}$, $i' \geq i$
- ▶ Μεταξύ των l συνεχόμενων ακεραίων $i, \dots, j - 1$, πρέπει να υπάρχει ένας που διαιρείται από το l .

Παραγοντοποίηση Pollard rho

- ▶ Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αλλά παίρνουμε $j = 2i$
- ▶ Αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i'} \equiv x_{2i'} \pmod{p}$, για όλα τα $i' \equiv 0 \pmod{l}$, $i' \geq i$
- ▶ Μεταξύ των l συνεχόμενων ακεραίων $i, \dots, j - 1$, πρέπει να υπάρχει ένας που διαιρείται από το l .
- ▶ Ο μικρότερος i' που ικανοποιεί τις παραπάνω συνθήκες είναι το πολύ $j - 1$

Παραγοντοποίηση Pollard rho

- ▶ Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αλλά παίρνουμε $j = 2i$
- ▶ Αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i'} \equiv x_{2i'} \pmod{p}$, για όλα τα $i' \equiv 0 \pmod{l}, i' \geq i$
- ▶ Μεταξύ των l συνεχόμενων ακεραίων $i, \dots, j - 1$, πρέπει να υπάρχει ένας που διαιρείται από το l .
- ▶ Ο μικρότερος i' που ικανοποιεί τις παραπάνω συνθήκες είναι το πολύ $j - 1$
- ▶ Επομένως, ο αριθμός επαναλήψεων είναι το πολύ j (που είναι το πολύ \sqrt{p})

Παραγοντοποίηση Pollard rho

- ▶ Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αλλά παίρνουμε $j = 2i$
- ▶ Αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i'} \equiv x_{2i'} \pmod{p}$, για όλα τα $i' \equiv 0 \pmod{l}$, $i' \geq i$
- ▶ Μεταξύ των l συνεχόμενων ακεραίων $i, \dots, j - 1$, πρέπει να υπάρχει ένας που διαιρείται από το l .
- ▶ Ο μικρότερος i' που ικανοποιεί τις παραπάνω συνθήκες είναι το πολύ $j - 1$
- ▶ Επομένως, ο αριθμός επαναλήψεων είναι το πολύ j (που είναι το πολύ \sqrt{p})
- ▶ Επειδή, $p < \sqrt{n}$, η αναμενόμενη πολυπλοκότητα είναι $O(n^{1/4})$ (

Παραγοντοποίηση Pollard rho

- ▶ Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αλλά παίρνουμε $j = 2i$
- ▶ Αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i'} \equiv x_{2i'} \pmod{p}$, για όλα τα $i' \equiv 0 \pmod{l}$, $i' \geq i$
- ▶ Μεταξύ των l συνεχόμενων ακεραίων $i, \dots, j - 1$, πρέπει να υπάρχει ένας που διαιρείται από το l .
- ▶ Ο μικρότερος i' που ικανοποιεί τις παραπάνω συνθήκες είναι το πολύ $j - 1$
- ▶ Επομένως, ο αριθμός επαναλήψεων είναι το πολύ j (που είναι το πολύ \sqrt{p})
- ▶ Επειδή, $p < \sqrt{n}$, η αναμενόμενη πολυπλοκότητα είναι $O(n^{1/4})$ (όχι μαθηματική απόδειξη!)

Παραγοντοποίηση Pollard rho

- ▶ Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αλλά παίρνουμε $j = 2i$
- ▶ Αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i'} \equiv x_{2i'} \pmod{p}$, για όλα τα $i' \equiv 0 \pmod{l}$, $i' \geq i$
- ▶ Μεταξύ των l συνεχόμενων ακεραίων $i, \dots, j - 1$, πρέπει να υπάρχει ένας που διαιρείται από το l .
- ▶ Ο μικρότερος i' που ικανοποιεί τις παραπάνω συνθήκες είναι το πολύ $j - 1$
- ▶ Επομένως, ο αριθμός επαναλήψεων είναι το πολύ j (που είναι το πολύ \sqrt{p})
- ▶ Επειδή, $p < \sqrt{n}$, η αναμενόμενη πολυπλοκότητα είναι $O(n^{1/4})$ (όχι μαθηματική απόδειξη!)
- ▶ Αποτυχία αλγορίθμου (πότε?, τι πιθανότητα?, τι κάνουμε?)

Παραγοντοποίηση Pollard rho

- ▶ Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αλλά παίρνουμε $j = 2i$
- ▶ Αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i'} \equiv x_{2i'} \pmod{p}$, για όλα τα $i' \equiv 0 \pmod{l}$, $i' \geq i$
- ▶ Μεταξύ των l συνεχόμενων ακεραίων $i, \dots, j - 1$, πρέπει να υπάρχει ένας που διαιρείται από το l .
- ▶ Ο μικρότερος i' που ικανοποιεί τις παραπάνω συνθήκες είναι το πολύ $j - 1$
- ▶ Επομένως, ο αριθμός επαναλήψεων είναι το πολύ j (που είναι το πολύ \sqrt{p})
- ▶ Επειδή, $p < \sqrt{n}$, η αναμενόμενη πολυπλοκότητα είναι $O(n^{1/4})$ (όχι μαθηματική απόδειξη!)
- ▶ Αποτυχία αλγορίθμου (πότε?, τι πιθανότητα?, τι κάνουμε?): όταν $x_i \equiv x_j \pmod{p}$ και $x_i \equiv x_j \pmod{n}$, με μικρή πιθανότητα (p/n)

Παραγοντοποίηση Pollard rho

- ▶ Βελτίωση: δε χρειάζεται να βρούμε την πρώτη σύγκρουση, αλλά παίρνουμε $j = 2i$
- ▶ Αν $x_i \equiv x_j \pmod{p}$, τότε $x_{i'} \equiv x_{2i'} \pmod{p}$, για όλα τα $i' \equiv 0 \pmod{l}$, $i' \geq i$
- ▶ Μεταξύ των l συνεχόμενων ακεραίων $i, \dots, j - 1$, πρέπει να υπάρχει ένας που διαιρείται από το l .
- ▶ Ο μικρότερος i' που ικανοποιεί τις παραπάνω συνθήκες είναι το πολύ $j - 1$
- ▶ Επομένως, ο αριθμός επαναλήψεων είναι το πολύ j (που είναι το πολύ \sqrt{p})
- ▶ Επειδή, $p < \sqrt{n}$, η αναμενόμενη πολυπλοκότητα είναι $O(n^{1/4})$ (όχι μαθηματική απόδειξη!)
- ▶ Αποτυχία αλγορίθμου (πότε?, τι πιθανότητα?, τι κάνουμε?): όταν $x_i \equiv x_j \pmod{p}$ και $x_i \equiv x_j \pmod{n}$, με μικρή πιθανότητα (p/n)
- ▶ Παρατήρηση: Σταθερό χώρο

Παραγοντοποίηση Pollard rho

Αλγόριθμος POLLARD RHO FACTORING (n)

$i = 1$

$x_1 \leftarrow \{0, 1, \dots, n - 1\}, y = x_1, k = 2$

while true

$i = i + 1$

$x_i = (f(x_{i-1})) \pmod{n}$

$d = \text{gcd}(y - x_i, n)$

if $d \neq 1$ and $d \neq n$

print d

if $i == k$

$y = x_i$

$k = 2k$

Παραγοντοποίηση Dixon

- ▶ Έστω $x \not\equiv \pm y \pmod{n}$, τ.ώ. $x^2 \equiv y^2 \pmod{n}$

Παραγοντοποίηση Dixon

- ▶ Έστω $x \not\equiv \pm y \pmod{n}$, τ.ώ. $x^2 \equiv y^2 \pmod{n}$
- ▶ Τότε

$$n \mid (x + y)(x - y)$$

αλλά $n \nmid (x + y)$, $n \nmid (x - y)$, άρα $\gcd(x + y, n)$ μη τετριμμένος διαιρέτης του n

Παραγοντοποίηση Dixon

▶ Έστω $x \not\equiv \pm y \pmod{n}$, τ.ώ. $x^2 \equiv y^2 \pmod{n}$

▶ Τότε

$$n \mid (x + y)(x - y)$$

αλλά $n \nmid (x + y)$, $n \nmid (x - y)$, άρα $\gcd(x + y, n)$ μη τετριμμένος διαιρέτης του n

▶ \mathcal{B} βάση παραγοντοποίησης: οι b μικρότεροι πρώτοι (b παράμετρος)

Παραγοντοποίηση Dixon

- ▶ Έστω $x \not\equiv \pm y \pmod{n}$, τ.ώ. $x^2 \equiv y^2 \pmod{n}$
- ▶ Τότε

$$n \mid (x + y)(x - y)$$

αλλά $n \nmid (x + y)$, $n \nmid (x - y)$, άρα $\gcd(x + y, n)$ μη τετριμμένος διαιρέτης του n

- ▶ \mathcal{B} βάση παραγοντοποίησης: οι b μικρότεροι πρώτοι (b παράμετρος)
- ▶ B -smooth: Βρίσκουμε ακεραίους z , τ.ώ. όλοι οι πρώτοι παράγοντες του $z^2 \pmod{n}$ να ανήκουν στο \mathcal{B}

Παραγοντοποίηση Dixon

- ▶ Έστω $x \not\equiv \pm y \pmod{n}$, τ.ώ. $x^2 \equiv y^2 \pmod{n}$
- ▶ Τότε

$$n \mid (x + y)(x - y)$$

αλλά $n \nmid (x + y)$, $n \nmid (x - y)$, άρα $\gcd(x + y, n)$ μη τετριμμένος διαιρέτης του n

- ▶ \mathcal{B} βάση παραγοντοποίησης: οι b μικρότεροι πρώτοι (b παράμετρος)
- ▶ B -smooth: Βρίσκουμε ακεραίους z , τ.ώ. όλοι οι πρώτοι παράγοντες του $z^2 \pmod{n}$ να ανήκουν στο \mathcal{B}
- ▶ Ιδέα: πάρε υποσύνολό τους, ώστε στο γινόμενο τους κάθε πρώτος παράγοντας του \mathcal{B} να χρησιμοποιείται άρτιο αριθμό φορές, δηλ.
 $(\prod z_i)^2 = (\prod b_j)^2 \pmod{n}$

Παραγοντοποίηση Dixon

Παράδειγμα. Έστω $n = 15770708441$, $b = 6$, τότε $\mathcal{B} = \{2, 3, 5, 7, 11, 13\}$

Έστω

$$8340934156^2 = 3 \times 7 \pmod{n}$$

$$12044942944^2 = 2 \times 7 \times 13 \pmod{n}$$

$$2773700011^2 = 2 \times 3 \times 13 \pmod{n}$$

Το γινόμενο τους δίνει:

$$(8340934156 \times 12044942944 \times 2773700011)^2 \equiv (2 \times 3 \times 7 \times 13)^2 \pmod{n}$$

Ισοδύναμα: $9503435785^2 \equiv 546^2 \pmod{n}$ και

$$\gcd(9503435785 - 546, 15770708441) = 115759$$

Παραγοντοποίηση Dixon

- ▶ Έστω $\mathcal{B} = \{p_1, p_2, \dots, p_b\}$ η βάση παραγοντοποίησης.

Παραγοντοποίηση Dixon

- ▶ Έστω $\mathcal{B} = \{p_1, p_2, \dots, p_b\}$ η βάση παραγοντοποίησης.
- ▶ Έστω $c > b$ στοιχεία $z_j^2 \equiv p_1^{a_{1j}} \times \dots \times p_b^{a_{bj}} \pmod{n}$, $1 \leq j \leq c$.

Παραγοντοποίηση Dixon

- ▶ Έστω $\mathcal{B} = \{p_1, p_2, \dots, p_b\}$ η βάση παραγοντοποίησης.
- ▶ Έστω $c > b$ στοιχεία $z_j^2 \equiv p_1^{a_{1j}} \times \dots \times p_b^{a_{bj}} \pmod{n}$, $1 \leq j \leq c$.
- ▶ Παίρνουμε τα $a_j = (a_{1j} \bmod 2, \dots, a_{bj} \bmod 2)$, δηλ. διανύσματα με 0,1.

Παραγοντοποίηση Dixon

- ▶ Έστω $\mathcal{B} = \{p_1, p_2, \dots, p_b\}$ η βάση παραγοντοποίησης.
- ▶ Έστω $c > b$ στοιχεία $z_j^2 \equiv p_1^{a_{1j}} \times \dots \times p_b^{a_{bj}} \pmod{n}$, $1 \leq j \leq c$.
- ▶ Παίρνουμε τα $a_j = (a_{1j} \bmod 2, \dots, a_{bj} \bmod 2)$, δηλ. διανύσματα με 0,1.
- ▶ Θέλουμε υποσύνολο διανυσμάτων, ώστε το άθροισμα τους mod 2 να είναι 0

Παραγοντοποίηση Dixon

- ▶ Έστω $\mathcal{B} = \{p_1, p_2, \dots, p_b\}$ η βάση παραγοντοποίησης.
- ▶ Έστω $c > b$ στοιχεία $z_j^2 \equiv p_1^{a_{1j}} \times \dots \times p_b^{a_{bj}} \pmod{n}$, $1 \leq j \leq c$.
- ▶ Παίρνουμε τα $a_j = (a_{1j} \bmod 2, \dots, a_{bj} \bmod 2)$, δηλ. διανύσματα με 0,1.
- ▶ Θέλουμε υποσύνολο διανυσμάτων, ώστε το άθροισμα τους mod 2 να είναι 0
- ▶ Δηλ. στο γινόμενο των αντίστοιχων z_j θα χρησιμοποιήσουμε κάποιους πρώτους του \mathcal{B} έναν άρτιο αριθμό φορές

Παραγοντοποίηση Dixon

- ▶ Έστω $\mathcal{B} = \{p_1, p_2, \dots, p_b\}$ η βάση παραγοντοποίησης.
- ▶ Έστω $c > b$ στοιχεία $z_j^2 \equiv p_1^{a_{1j}} \times \dots \times p_b^{a_{bj}} \pmod{n}$, $1 \leq j \leq c$.
- ▶ Παίρνουμε τα $a_j = (a_{1j} \bmod 2, \dots, a_{bj} \bmod 2)$, δηλ. διανύσματα με 0,1.
- ▶ Θέλουμε υποσύνολο διανυσμάτων, ώστε το άθροισμα τους mod 2 να είναι 0
- ▶ Δηλ. στο γινόμενο των αντίστοιχων z_j θα χρησιμοποιήσουμε κάποιους πρώτους του \mathcal{B} έναν άρτιο αριθμό φορές
- ▶ Εύρεση υποσυνόλου γραμμών ενός πίνακα, ώστε το άθροισμα τους να είναι το διάνυσμα $\vec{0}$:

Παραγοντοποίηση Dixon

- ▶ Έστω $\mathcal{B} = \{p_1, p_2, \dots, p_b\}$ η βάση παραγοντοποίησης.
- ▶ Έστω $c > b$ στοιχεία $z_j^2 \equiv p_1^{a_{1j}} \times \dots \times p_b^{a_{bj}} \pmod{n}$, $1 \leq j \leq c$.
- ▶ Παίρνουμε τα $a_j = (a_{1j} \bmod 2, \dots, a_{bj} \bmod 2)$, δηλ. διανύσματα με 0,1.
- ▶ Θέλουμε υποσύνολο διανυσμάτων, ώστε το άθροισμα τους mod 2 να είναι 0
- ▶ Δηλ. στο γινόμενο των αντίστοιχων z_j θα χρησιμοποιήσουμε κάποιους πρώτους του \mathcal{B} έναν άρτιο αριθμό φορές
- ▶ Εύρεση υποσυνόλου γραμμών ενός πίνακα, ώστε το άθροισμα τους να είναι το διάνυσμα $\vec{0}$: Gauss, εύκολα

Παραγοντοποίηση Dixon

Εύρεση των z_j :

- ▶ Τυχαίοι αριθμοί (Random Squares algorithm)
- ▶ $j + \lceil \sqrt{kn} \rceil, j = 0, 1, 2, \dots, k = 1, 2, \dots$
- ▶ $\lfloor \sqrt{kn} \rfloor$

Παραγοντοποίηση Dixon

- ▶ Πόσο μεγάλο πρέπει να είναι το B ; Πολύ μεγάλο, καλύτερη πιθανότητα να βρούμε παράγοντα, αλλά και περισσότερο χρόνο να βρούμε υποσύνολο με άθροισμα $\vec{0}$
- ▶ Αναμενόμενη χρονική πολυπλοκότητα $O(2^c \sqrt{n \log \log n})$ (υποεκθετικός)

Παραγοντοποίηση: άλλες μέθοδοι

Πρακτικά χρησιμοποιούνται οι:

1. Quadratic sieve: μια ειδική διαδικασία “κόσκινου” για την επιλογή των z_j
2. Number field sieve (ο πιο γρήγορος, $O(e^{(1.92+o(1))(\ln n)^{1/3}(\ln \ln n)^{2/3}})$)