თუ გავითვალიწინებთ ქვემოთ მოყვანილ წყვილებს (იწყება მეორე გვერდიდან)და შევეცდებით მოვიფიქროთ რაიმე წესი, პირობა, რისი გათვალისწინებისას (მატრიცის აშენების პროცესში) ჩვენ მოვხვდებით აუცილებლად ამ წყვილების სიმრავლეში (თუ ამ წყვილების სიმრავლეშ ვერ მოვხვდებით ესეიგი ვერ მოხდება დაშიფვრა დეშიფრაცია). შესაბამისად შესაძლებელი მატრიცების რაოდენობა იქნება ძალიან მცირე. კერძოდ მხოლოდ იმდენი ვარიანტი რამდენი წყვილიც გვაქვს და სავარაუდოდ მათი წრფივი კომბინაციები.(საჭიროებს დაზუსტებას).

ასევე თუ დავაკვირდებით ტენდენციას სიმრავლე იზრდება და იმის და მიუხედავად რო პირდაპირ არ ჩანს კორელაცია P-ს ზრდასა და სიმრავლის ზრდას შორის. (რადგან ზოგ შემთხვევაში იგივეა, ზოგში ნაკლები ზოგში მეტი მაგრამ მაინც იზრდება.) დავინახავთ რომ ბევრ წინა რიცხვს მოიცავს. P.S იგივე პრინციპი არის დიფი-ჰელმანში. იქაც იგივე სიმრავლიდან ვარჩევთ.

შესაბამისად ჯერ ერთი თითქმის შეუძლებელია რაიმე ზოგადი პრინციპის მოფიქრება და პირობის რომ მატრიცა მოხვდეს ამ სიმრავლეში და მეორე თუ დავუშვებთ რომ P არის ძალიან დიდი რიცხვი, იზრდება ალბათბა რომ რანაირი გადაუგვარებელ-კომუტატიურ მატრიცათა სიმრავლეც არ უდნა შევადგინოთ მიღებული ვექტორი მოხვდება იმ დიდი მარტივი რიცხვის წყვილების სიმრავლეში. შესაბამისად e სტრიქონსაც შემთხვევითად ავირჩევთ, და დიდი ალბათბით გვექნება გასაღებები. თუ არ გამოვა იმის გამო რომ დიდი სიმრავლე გვაქვს მინიმალური ახალი მატრიცების გენერირებითაც აუცილებლად მოვხვდებით სიმრავლეში.

პატარაი რიცხვებზე არ გამოდის და თითქმის დარწმუნებული ვარ რომ ზოგადი პრინციპის შედგენაც შეუძლებელია და არც არის საჭირო. რადგან ჩვენი გასაღებების მნიშვნელობები მკაცრად განსაზღვრულია.

ასევე არ შემიძლია არ ავღნიშნო რომ გადავაწყდი კიდევ ერთ პრობლემას. კერძოდ

სიმრავლის გაზრდის მიზნით დიდი მარტივი რიცხვიდან ავარჩიე წყვილები. მივყევი ყველა ნაიჯს და აღმოვაჩინე რომ დიდი გამოთვლების დროს ხელსაწყო ჩვენთვის დიდი ხნის ნაცნობი OVERFLOW პრობლემას აწყდება და ვერ ახდენს გადაცემული რიცხვების ხარისხებიდან ნაშთის სწორად პოვნას. სავარაუდოდ ამას რაიმე სახის გადაწყვეტა ექნება. რომელზეც ბევრი არ მიფიქრია მაგრამ აღსანიშნავია რომ ასეთ პრობლემასაც შეიძლება გადავაწყდეთ.

(1; 100) შუალედში ყველა მარტივი P რიცხვისთვის ყველა სავარაუდო AB წყვილი რიცხვები რომლებიც აკმაყოფილებენ განტოლებას: AB = 1 mod(P)

For Prime : 2

Total 0 pairs.

For Prime : 3

i = 1 j = 1

Total 1 pairs.

For Prime : 5

i = 1 j = 1

i = 3 j = 3

Total 2 pairs.

For Prime : 7

i = 1 j = 1

i = 5 j = 5

Total 2 pairs.

For Prime : 11

i = 1 j = 1

i = 3 j = 7

i = 9 j = 9

Total 3 pairs.

For Prime : 13

i = 1 j = 1

i = 5 j = 5

i = 7 j = 7

i = 11 j = 11

Total 4 pairs.

For Prime : 17

i = 1 j = 1

i = 3 j = 11

i = 5 j = 13

i = 7 j = 7

i = 9 j = 9

i = 15 j = 15

Total 6 pairs.

For Prime : 19

i = 1 j = 1

i = 5 j = 11

i = 7 j = 13

i = 17 j = 17

Total 4 pairs.

For Prime : 23

i = 1 j = 1

i = 3 j = 15

i = 5 j = 9

i = 7 j = 19

i = 13 j = 17

i = 21 j = 21

Total 6 pairs.

For Prime : 29

i = 1 j = 1

i = 3 j = 19

i = 5 j = 17

i = 9 j = 25

i = 11 j = 23

i = 13 j = 13

i = 15 j = 15

i = 27 j = 27

Total 8 pairs.

For Prime : 31

i = 1 j = 1

i = 7 j = 13

i = 11 j = 11

i = 17 j = 23

i = 19 j = 19

i = 29 j = 29

Total 6 pairs.

For Prime : 37

i = 1 j = 1

i = 5 j = 29

i = 7 j = 31

i = 11 j = 23

i = 13 j = 25

i = 17 j = 17

i = 19 j = 19

i = 35 j = 35

Total 8 pairs.

For Prime : 41

i = 1 j = 1

i = 3 j = 27

i = 7 j = 23

i = 9 j = 9

i = 11 j = 11

i = 13 j = 37

i = 17 j = 33

i = 19 j = 19

i = 21 j = 21

i = 29 j = 29

i = 31 j = 31

i = 39 j = 39

Total 12 pairs.

For Prime : 43

i = 1 j = 1

i = 5 j = 17

i = 11 j = 23

i = 13 j = 13

i = 19 j = 31

i = 25 j = 37

i = 29 j = 29

i = 41 j = 41

Total 8 pairs.

For Prime : 47

i = 1 j = 1

i = 3 j = 31

i = 5 j = 37

i = 7 j = 33

i = 9 j = 41

i = 11 j = 21

i = 13 j = 39

i = 15 j = 43

i = 17 j = 19

i = 25 j = 35

i = 27 j = 29

i = 45 j = 45

Total 12 pairs.

For Prime : 53

i = 1 j = 1

i = 3 j = 35

i = 5 j = 21

i = 7 j = 15

i = 9 j = 29

i = 11 j = 19

i = 17 j = 49

i = 23 j = 43

i = 25 j = 25

i = 27 j = 27

i = 31 j = 47

i = 33 j = 41

i = 37 j = 45

i = 51 j = 51

Total 14 pairs.

For Prime : 59

i = 1 j = 1

i = 3 j = 39

i = 5 j = 35

i = 7 j = 25

i = 9 j = 13

i = 11 j = 37

i = 15 j = 31

i = 17 j = 41

i = 19 j = 55

i = 21 j = 47

i = 23 j = 53

i = 27 j = 43

i = 33 j = 51

i = 45 j = 49

i = 57 j = 57

Total 15 pairs.

For Prime : 61

i = 1 j = 1

i = 7 j = 43

i = 11 j = 11

i = 13 j = 37

i = 17 j = 53

i = 19 j = 19

i = 23 j = 47

i = 29 j = 29

i = 31 j = 31

i = 41 j = 41

i = 49 j = 49

i = 59 j = 59

Total 12 pairs.

For Prime : 67

i = 1 j = 1

i = 5 j = 53

i = 7 j = 19

i = 13 j = 61

i = 17 j = 35

i = 23 j = 23

i = 25 j = 37

i = 29 j = 41

i = 31 j = 49

i = 43 j = 43

i = 47 j = 59

i = 65 j = 65

Total 12 pairs.

For Prime : 71

i = 1 j = 1

i = 3 j = 47

i = 9 j = 39

i = 11 j = 51

i = 13 j = 27

i = 17 j = 33

i = 19 j = 59

i = 23 j = 67

i = 29 j = 29

i = 31 j = 61

i = 37 j = 53

i = 41 j = 41

i = 43 j = 57

i = 69 j = 69

Total 14 pairs.

For Prime : 73

i = 1 j = 1

i = 5 j = 29

i = 7 j = 31

i = 11 j = 59

i = 13 j = 61

i = 17 j = 17

i = 19 j = 19

i = 23 j = 47

i = 25 j = 49

i = 35 j = 35

i = 37 j = 37

i = 41 j = 65

i = 43 j = 67

i = 53 j = 53

i = 55 j = 55

i = 71 j = 71

Total 16 pairs.

For Prime : 79

i = 1 j = 1

i = 5 j = 47

i = 7 j = 67

i = 11 j = 71

i = 17 j = 23

i = 19 j = 37

i = 25 j = 25

i = 29 j = 35

i = 31 j = 73

i = 41 j = 59

i = 43 j = 49

i = 53 j = 53

i = 55 j = 61

i = 77 j = 77

Total 14 pairs.

For Prime : 83

i = 1 j = 1

i = 3 j = 55

i = 5 j = 33

i = 7 j = 47

i = 9 j = 73

i = 11 j = 15

i = 13 j = 19

i = 17 j = 29

i = 21 j = 43

i = 23 j = 25

i = 27 j = 79

i = 31 j = 45

i = 35 j = 75

i = 37 j = 51

i = 39 j = 61

i = 49 j = 77

i = 53 j = 65

i = 57 j = 59

i = 63 j = 69

i = 67 j = 71

i = 81 j = 81

Total 21 pairs.

For Prime : 89

i = 1 j = 1

i = 3 j = 59

i = 5 j = 53

i = 7 j = 63

i = 9 j = 49

i = 13 j = 61

i = 15 j = 47

i = 17 j = 57

i = 19 j = 51

i = 21 j = 21

i = 23 j = 23

i = 25 j = 81

i = 27 j = 75

i = 29 j = 85

i = 31 j = 71

i = 35 j = 83

i = 37 j = 69

i = 39 j = 79

i = 41 j = 73

i = 43 j = 43

i = 45 j = 45

i = 65 j = 65

i = 67 j = 67

i = 87 j = 87

Total 24 pairs.

For Prime : 97

i = 1 j = 1

i = 5 j = 77

i = 7 j = 55

i = 11 j = 35

i = 13 j = 37

i = 17 j = 17

i = 19 j = 91

i = 23 j = 71

i = 25 j = 73

i = 29 j = 53

i = 31 j = 31

i = 41 j = 89

i = 43 j = 67

i = 47 j = 47

i = 49 j = 49

i = 59 j = 83

i = 61 j = 85

i = 65 j = 65

i = 79 j = 79

i = 95 j = 95

Total 20 pairs.