

# Strong passwords

More and more of our daily life takes place online. To confirm our identity online services often require a password. However, these services are often not satisfied with just any password. This is, of course, completely justified. Usually several conditions are imposed in order to prevent passwords from being easily guessed. A password provides strong protection if all of the following conditions are met.

- The password is at least 8 characters long,
- the password contains at least one uppercase letter,
- the password contains at least one lowercase letter,
- the password contains at least one digit,
- the password contains at least one special character that is not a letter or a digit.

If three or four of these conditions apply, the password provides moderate protection, and if less than three conditions are met it provides weak protection.

## Input

The first line of the input contains an integer  $t$  ( $1 \leq t \leq 100$ ) which indicates how many test cases there are. This is followed by  $t$  lines, each containing one password.

## Output

For each password one of the words must be printed as strong, moderate or weak, as an indication of the strength of the password protection.

## Example

### Input:

```
3
password
Prog2011
five+1=SIX
```

### Output:

```
weak
moderate
strong
```

Steeds meer van ons dagelijks leven speelt zich online af. Om onze identiteit te bevestigen vragen online diensten vaak om een wachtwoord op te geven. Deze diensten zijn vaak echter niet zomaar tevreden met eender welk wachtwoord. Dit geheel terecht. Meestal worden enkele voorwaarden opgelegd om te verhinderen dat wachtwoorden makkelijk zouden kunnen geraden worden. Een wachtwoord geeft een sterke bescherming als elk van de volgende voorwaarden voldaan zijn

- het wachtwoord is minstens 8 karakters lang,

- het wachtwoord bevat minstens één hoofdletter,
- het wachtwoord bevat minstens één kleine letter,
- het wachtwoord bevat minstens één cijfer,
- het wachtwoord bevat minstens één speciaal karakter dat geen letter of cijfer is.

Indien drie of vier van deze voorwaarden gelden, geeft het wachtwoord een matige bescherming, en als er minder dan drie voorwaarden voldaan zijn, dan geeft het wachtwoord een zwakke bescherming.

## Invoer

De eerste regel van de invoer bevat een natuurlijk getal  $t$  ( $1 \leq t \leq 100$ ) dat aangeeft hoeveel testgevallen er zijn. Daarna volgen  $t$  regels die elk één wachtwoord bevatten.

## Uitvoer

Voor elk wachtwoord moet één van de woorden sterk, matig of zwak uitgeschreven worden, als aanduiding van de sterkte van bescherming van het wachtwoord.

## Voorbeeld

### Invoer:

3  
wachtwoord  
Prog2011  
vijf+1=ZES

### Uitvoer:

zwak  
matig  
sterk